IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of	)
	)
TAKEDA et al.	)
	)
Application Number: To be Assigned	)
	)
Filed: Concurrently Herewith	)
	)
For: SERVER, TERMINAL CONTROL DEVICE AND TERMINAL AUTHENTICATION METHOD	)
	)
ATTORNEY DOCKET NO. HITA.0506	)

Honorable Assistant Commissioner
for Patents
Washington, D.C. 20231

REQUEST FOR PRIORITY
UNDER 35 U.S.C. § 119
AND THE INTERNATIONAL CONVENTION

Sir:

In the matter of the above-captioned application for a United States patent, notice is hereby given that the Applicant claims the priority date of March 11, 2003, the filing date of the corresponding Japanese patent application 2003-064329.

A certified copy of Japanese patent application 2003-064329 is being submitted herewith. Acknowledgment of receipt of the certified copy is respectfully requested in due course.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344

Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200
February 23, 2004

310300060 HP

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月１１日

出願番号
Application Number: 特願２００３－０６４３２９

[ST. 10/C]: ［ＪＰ２００３－０６４３２９］

出願人
Applicant(s): 株式会社日立製作所

２００３年　９月２６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０７９３９９

【書類名】　特許願

【整理番号】　H03000601A

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/22

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内

【氏名】　武田　幸子

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内

【氏名】　井内　秀則

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内

【氏名】　鈴木　伸介

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内

【氏名】　竹内　敬亮

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【電話番号】　03-3212-1111

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　サーバ装置、端末制御装置及び端末認証方法

【特許請求の範囲】

【請求項１】

公開鍵証明書を発行及び保証する手段と、

端末装置に対するIPv6 Prefix配布可否情報を保持する手段と、

端末装置から公開鍵証明書発行要求を受信し、前記端末装置のPrefix配布可否情報を更新する手段とを備え、

前記端末装置から公開鍵証明書発行要求を受信して、前記端末装置の公開鍵証明書を発行し、前記Prefix配布可否情報を更新し、前記端末装置に対して前記証明書を送信することを特徴とするサーバ装置。

【請求項２】

請求項１に記載のサーバ装置において、

Prefix配布機能を有する情報処理装置との通信手段を備え、

前記情報処理装置からPrefix配布可否の問い合わせを受信し、前記端末装置のPrefix配布可否情報を検索し、得られた情報を前記情報処理装置に対して送信することを特徴とするサーバ装置。

【請求項３】

請求項１に記載のサーバ装置において、

端末装置の位置情報を管理する端末制御装置との通信手段を備え、

前記端末制御装置からPrefix配布可否の問い合わせを受信し、前記端末装置のPrefix配布可否情報を検索し、得られた情報を前記端末制御装置に対して送信することを特徴とするサーバ装置。

【請求項４】

公開鍵証明書を発行及び保証する機能とPrefix配布許可情報とを備えるサーバ装置との通信手段と、前記サーバ装置から公開鍵証明書を取得する手段と、IPsecによるセキュリティを確保する手段と、端末装置の位置情報を格納する手段とを備え、

端末装置から本人性確認信号を受信し、前記端末装置の公開鍵証明書を取得す

ることを特徴とする端末制御装置。

【請求項５】

請求項４記載の端末制御装置において、Prefix配布機能を有する情報処理装置との通信手段とを備え、

前記末装置から前記本人確認性信号を受信し、前記情報処理装置に対しPrefix情報を問合せ、前記情報処理装置が前記Prefix情報を配布していれば、前記本人性確認信号の応答を前記端末装置に対して送信することを特徴とする端末制御装置。

【請求項６】

請求項４または請求項５に記載の端末制御装置において、

前記端末装置から位置登録要求を受信し、前記端末装置のセキュリティ情報を読み出し、前記要求が前記セキュリティ情報に合致すれば前記端末装置の位置登録処理を行うことを特徴とする端末制御装置。

【請求項７】

請求項４から請求項６のいずれか１項に記載の端末制御装置において、

前記サーバ装置から前記端末装置のPrefix配布許可情報を読み出し、前記サーバ装置が前記端末装置に対してPrefixの配布を許可すれば、前記端末装置にPrefix情報を広告することを特徴とする端末制御装置。

【請求項８】

在圏網と、該在圏網に接続可能な端末装置と、該端末装置が属しかつ前記在圏網と相互接続されるホーム網と、該ホーム網に設置された端末制御装置と、公開鍵証明書を発行及び保証する手段を備えたサーバ装置と、Prefix配布機能を備える情報処理装置とを備えた通信システムにおける端末認証方法において、

前記サーバ装置は前記端末装置に対して公開鍵証明書を発行し、前記端末装置のPrefix配布情報を更新し、

前記情報処理装置は、

前記端末装置からPrefix配布要求を受信し、前記サーバ装置に前記端末装置のPrefix配布可否情報を問合せ、Prefixの配布が許可される場合前記端末装置にPrefix情報を配布し、

前記端末制御装置は、

前記端末装置から本人性確認信号を受信し、前記端末装置のPrefix情報を前記情報処理装置に送信し、

前記情報処理装置は、前記Prefix情報を発行した端末装置と前記端末制御装置との間にセキュリティアソシエーションを確立することを特徴とする端末認証方法。

【請求項９】

請求項8に記載の端末認証方法において、前記ホーム網と前記在圏網を相互接続する通信装置が前記情報処理装置にPrefix配布要求を送信することを特徴とする端末認証方法。

【請求項１０】

請求項８または請求項９に記載の端末認証方法において、

前記端末制御装置は、前記端末装置から位置登録要求を受信し、前記セキュリティアソシエーションを読み出し、前記位置登録要求が前記セキュリティアソシエーションを満たす場合に前記端末装置の位置登録を許可することを特徴とする端末認証方法。

【請求項１１】

請求項８から請求項１０のいずれか１項に記載の端末認証方法において、前記端末制御装置は、前記サーバ装置との通信手段と、端末装置の公開鍵証明書情報を格納する手段とを備え、

前記移動体通信装置は、前記サーバ装置が許可した端末装置に対してPrefix情報を送信することを特徴とする端末認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、サーバ装置、移動体制御装置、および、端末認証方法に関する。特にモバイルＩＰ（Mobile IP）プロトコルを適用した通信システムにおける、公開鍵証明書の発行・保証を行うサーバ装置、ホームエージェント装置、および、端末認証方法に関する。

【０００２】

【従来の技術】

IETF(Internet Engineering Task Force)は、Mobile IPv6の仕様を検討している（Ref. Mobility Support in IPv6 <draft-ietf-mobileip-ipv6-19.txt>、 Work in Progress）。

Mobile IPv6の網構成要素は、移動ノード（MN：Mobile Node）、ホームエージェント（HA：Home Agent）、通信相手（CN：Correspondent Node）である。

MNには移動しても変わることのない一意のIPアドレス（ホームアドレス）が付与される。ホームアドレスと同じプレフィックスを持つリンクをホームリンクと呼ぶ。HAはホームリンク以外に存在するMNの位置情報（Binding Cache）を管理する。

【０００３】

MNはホームリンク以外のリンク（在圏リンク）において気付アドレス（Care of Address、以下CoAで表す）を取得する。ホームリンク以外に存在するMNは、在圏リンクに存在するルータが定期的に送信するルータ広告を受信する。MNはホームアドレスと異なるプレフィックスを検出することで移動を検知してCoAを生成する。MNはHAにホームアドレスとCoAの対応情報を登録する。

【０００４】

MNは、Home Agent Address Discovery機能（HAアドレス発見機能）を備え、HAのIPアドレスを動的に検索してもよい。まず、MNはホームリンクのプレフィックスからMobile IPv6 Home-Agents Anycast Addressを作成する。MNは上記アドレス宛にHAアドレス発見要求（ICMP Home Agent Address Discovery Request）を送信する。上記信号は、ホームリンクのいずれかのHAが受信する。上記信号を受信したHAは、MNに対してHAの情報を含むHAアドレス発見応答（ICMP Home Agent Address Discovery Reply）を送信する。MNは上記信号からHAの情報を取り出し、HAのアドレスを取得する。MNは上記HAアドレスに対して位置登録信号（Binding Update）を送信する。

【０００５】

HAは、上記信号（Binding Update）を受信し、MNの位置情報をBinding Cache

に格納する。

【０００６】

次に、HAはMNのプロキシとして動作するため、MNの代わりにNeighbor Advertisementをホームリンクのall-nodes multicastアドレス宛に送信する。上記Neighbor Advertisementを受信したノードは、Neighbor Cacheに、MNのホームアドレスとHAのリンクレイヤアドレスの対応情報を格納する。HAは、MNのホームアドレス宛に送信されたパケットを捕捉する。

【０００７】

Mobile IPv6は、ホームリンク以外に存在するMNに対して、ホーム網のプレフィックス情報を通知する機能を備える。例えば、ホーム網がプレフィックスを変更する場合、HAはBinding Cacheを参照して位置登録中のMNにプレフィックス情報を通知（Mobile Prefix Advertisement）する。MNはHAにプレフィックス情報を要請（Mobile Prefix Solicitation）してもよい。

【０００８】

IP網上のセキュリティを実現する技術として、IP Security Protocol(IPsec)が注目されている。IPsecは、暗号化技術や認証技術を使用して、IPパケットを安全に運ぶ技術である。Mobile IPv6は、MNがHAに送信する位置登録信号にIPsecを適用する（Ref. draft-ietf-mobileip-mipv6-ha-ipsec-01.txt、 Work in Progress）。

【０００９】

IPsecは、IPsecを適用する装置の間にSA（Security Association）を生成することによってセキュリティ機能を提供する。IPsecを適用する装置は、SPD（Security Policy Database）とSAD(Security Assosiation Database)を備える。

【００１０】

SPDはパケットの処理方法を規定する。SADは、IPsec適用装置が保持するSAのリストである。SAはSPI（Seculity Parameters Index）で識別する。

【００１１】

SAの生成方法には、手動設定する方法と自動生成する方法がある。IKE（Internet Key Exchange）は、SAを自動生成・管理するプロトコルである。IKEは、Pro

posal交換機能と、秘密対称鍵を生成する機能と、IKE通信相手の認証機能とを用いてSAを自動生成する。

【００１２】

IKE通信相手の認証方式には、Pre-Shared Key認証方式、公開鍵暗号認証方式、デジタル署名認証方式等が規定されている。デジタル署名認証方式は、通信相手毎に事前に鍵情報等を共有する必要がないため、拡張性が高い。デジタル署名認証方式は、CA（Certification Authority）が発行する公開鍵証明書を使用する。公開鍵証明書のフォーマットは、X.509で規定される。

【００１３】

CMP（Certificate Managemnet Protocol）は、電子証明書を発行・管理するプロトコルである。CMPは、IETF RFC2510で規定される。CMPは、トランスポートプロトコルにHTTP(HyperText Transfer Protocol)やTCP(Transmission Control Protocol)を利用する。

【００１４】

一方、Mobile IPv6をベースに局所的な移動管理を行う技術として、Hierarchical Mobile IPv6 mobility management（HMIPv6）(Ref. draft-ietf-mobileip-hmipv6-07.txt、Work in Progress)が提案されている。

HMIPv6は、HAとMNの間にMAP(Mobile Anchor Point)を備える。MNは、AR（Access Router）からMAPオプションを含むルータ広告を受信して、MAPのIPアドレスを取得し、地域気付アドレス（Regional Core of Address：RCoA）とリンク気付アドレス（On-link CoA：LCoA）を生成する。HMIPv6対応MNは、MAPとHAに位置登録を行う。MAPはMNのRCoAとLCoAのバインディング情報を管理する。HAはMNのホームアドレスとRCoAのバインディング情報を管理する。MNがMAP内で移動した場合、MNはMAPの位置情報のみ更新する。

IETFは、IPv6 Prefix Delegation Options for DHCPv6（以下、DHCP-PD）(draft-ietf-dhc-dhcpv6-opt-prefix-delegation-01.txt、Work in Progress）を検討している。DHCP-PDは、DHCP(Dynamic Host Configuration Protocol)を活用して、アドレス割当側からサイトにIPv6プレフィックス（群）を割り当てる機能である。

DHCP-PDの構成要素は、Delegating RouterとRequesting Routerである。Requesting RouterがDelegating RouterにIPv6プレフィックス（群）の割り当てを要求する。Delegating RouterはIPv6プレフィックス（群）を選択して、それをRequesting Routerに送信する。DHCP-PDは、例えば、ISP（Internet Service Provider）が加入者にPrefixを割り当てるとき利用される。

【００１５】

【発明が解決しようとする課題】

領域Aと領域Bが相互接続された通信システムにおいて、領域Aに属する移動ノード（MN）が領域Bに移動した場合、MNは領域Aに存在するHAに位置登録を行う。位置登録信号には、IPsecを適用する。

【００１６】

HAとMNの間にSAを手動設定すると、暗号化などに使用する鍵が漏洩した場合、安全性が保てないという課題がある。また、Mobile IPv6のプレフィックス通知機能やHAアドレス発見機能を使用すると、MNのホームアドレス、或いは、HAアドレスが変わる。このため、MNとHA間のSAを手動設定する方法は、システムの運用上現実的ではない。さらに、現状のMobile IPには、MNの正当性を確認する手段がない。

【００１７】

本特許の目的は、Mobile IPの技術を活用して、端末の認証方法を提供することにある。

特に、デジタル署名認証方法とMobile IPの位置登録手順を連携し、HAが公開鍵証明書にリンクしたホームアドレスに対してSAを生成・保持することにより、端末に対する認証手順を提供する。

【００１８】

本発明のその他の目的は、MNがホームアドレスを動的に取得する場合、DHCP-PD Delegating RouterとCAの連携と、及び、DHCP-PD Delegating RouterとHAの連携により、端末の正当性を確認する認証手順を提供することにある。

【００１９】

特に、領域Aに属するHAをホーム網とする端末xが、領域BにおいてDHCP-PD機能

を活用してホーム網のプレフィックスを取得する場合、以下を目的とする。

１）DHCP-PD Delegating Routerは、CAが許可した端末に対してPrefix情報を配布する。

２）HAは、上記Delegating Routerが配布したPrefixをもつIPアドレスに対してSAを生成し、上記SAを満たす位置登録を許容する。

【００２０】

本発明のその他の目的は、領域Bに属する通信装置がHMIPv6対応MAPであり、上記通信装置が、MNから制御信号（Binding Update）を受信してDHCP-PD機能を起動する場合、DHCP Delegating Routerは、CAが許可した端末に対してPrefix情報を配布する認証方法を提供することにある。

【００２１】

本発明のその他の目的は、HAはCAが許可した端末に対してプレフィックス情報を広告する通信方法を提供することにある。

【００２２】

【課題を解決するための手段】

上記の問題を解決するために、本発明は、従来の認証方式に加えて少なくても以下の手段を備える。すなわち、

（１）CAはDHCP-PD Delegating Router機能との通信手段を備える。また、CAは、端末に対して公開鍵証明書を発行し、Prefix情報の通知を許可する。

（２）端末は、Mobile IPv6機能と、IPsec機能と、デジタル署名に必要な情報を保持する機能を備える。デジタル署名認証に必要な情報は、外部記憶装置から受信してもよい。端末は、移動端末でなくてもよい。

（３）端末制御装置は、DHCPv6 Prefix Delegation Option（以下、DHCP-PD）のDelegating Router機能を備える。Delegating Router機能は、CAとの通信手段と、CAが許可した端末に対してPrefix情報を通知する手段を備える。

（４）端末制御装置は、端末からSAの生成要求を受信すると、上記DHCP-PD Delegating 機能にPrefix情報を問い合わせる。上記Delegating Router機能が配布したPrefixを利用する端末であれば、端末制御装置は上記端末との間にSAを生成する手段を備える。

（５）あるいは、端末制御装置が端末の公開鍵証明書を保持する手段を備え、CAが許可した端末に対してPrefix情報を通知してもよい。

【００２３】

【発明の実施の形態】

（実施例１）

本発明の第１の実施の形態を図面を用いて説明する。なお、本実施例においては、HAが端末制御装置に該当する。

【００２４】

代表例として、Mobile IPv6対応移動ノード（MN）がホームリンク（以下、ホーム網）以外の網（以下、在圏網）に存在するとき、MNの認証方法及び位置登録方法について詳細に説明する。

【００２５】

図１は、本発明における通信網の構成例を示す。通信網はMN4のホーム網8とIP網７と在圏網5（5a、5b）から構成される。実施例において、ホーム網8、IP網７、及び、在圏網5はIPv6網である。MN4はMobile IPv6対応移動ノード（MN）である。情報家電端末9は、Mobile IPv6対応MNの機能を備える。在圏網5とIP網７、及び、IP網７とホーム網8は、ルータ、或いは、ゲートウェイ装置を介して接続される。在圏網５とホーム網8は、ルータ、或いは、ゲートウェイ装置を介して直接接続してもよい。

ホーム網8は、HA１を備える。HA１はMobile IPv6対応ホームエージェント（HA）である。HA1はホーム網8以外に存在するMNの位置情報を管理する。

在圏網5（5a、5b）は通信装置2（2a、2b）とルータ6(6a、6b、6c、6d)を備える。通信装置2は、ルータ6とのインタフェースと、IP網7とのインタフェースを備える。ルータ6は機器認証機能を備える。

ルータ6が機器認証機能を備える代わりに、ルータ6に機器認証機能を備えるサーバとの通信手段を備えてもよい。

IP網7はCA3を備える。ホーム網8或いは在圏網5がCA3を備えてもよい。

【００２６】

図２はMN4のホーム網8に設置するHA1の構成例を示す。HA1は、サーバ部11（11

a、11b、）、サーバ部12と、回線18（18a、18b、18m、18n）を収容するインタフェース部（IF）19（19a、19b、19m、19n）と、スイッチ部17(17a、17b)とから構成される。

【００２７】

サーバ部11は、主にパケット送信・受信処理部13と、IPsec処理部14と、Mobile IP処理部15とを備える。

パケット送信・受信処理部13はデータパケットを送信又は受信する機能を備える。

IPsec処理部14は、主にSPDとSADとIPsec処理ルーチン70を備え、パケットの認証処理や暗号化処理を行う。また、IPsec処理部14は、CA3からサーバ部11の公開鍵証明書を取得する。

Mobile IP処理部15は、Mobile IPv6のホームエージェント（HA）機能を備える。

Mobile IP処理部15は、Binding Cache管理テーブル310を含む。

【００２８】

図３はBinding Cache管理テーブル310のテーブル構成の一例を示す。Binding Cache管理テーブル310は、MNのホームアドレス311に対して、少なくてもMNが在圏網で取得したCare of Address (CoA)312と、Binding Cacheの有効期間を示すLifetime313の対応関係を格納する。

【００２９】

サーバ部12は、主にパケット送信・受信処理部13と、DHCP PD機能部16とを備える。

【００３０】

DHCP PD機能部16は、DHCP-PD Delegating Router機能を備え、主にPrefix管理テーブル320と、Prefix Delegation処理ルーチン60と、DHCP-PDを識別するIA_PDとMNの識別子の対応テーブルとを含む。

【００３１】

図４はPrefix管理テーブル320のテーブル構成の一例を示す。Prefix管理テーブル320は、DHCP Client識別子321に対して、少なくてもPrefix（群）を示すIAID322と、配布したPrefix323と、PrefixのLifetime324との対応関係を格納する。

本実施例において、サーバ部12のDHCP-PD機能はHA１に実装されるが、HA１とは別のサーバ装置に、DHCP－PD機能を実装してもよい。

【００３２】

図７はIP網7に設置する認証局（CA）3の構成例を示す。CA3は、CPU31と、メモリ32と、回線34を収容するインタフェース部（IF）33とをバス35で接続する構成をとる。

メモリ32は、少なくてもPrefix配布管理テーブル330と、公開鍵証明書発行ルーチン80と、証明書情報格納テーブルとを備える。

【００３３】

図８はPrefix配布管理テーブル330のテーブル構成の一例を示す。Prefix配布管理テーブル330は、端末の識別子（ID）331に対してPrefix発行許可か否かを示すフラグ332の対応関係を格納する。

【００３４】

図１７と図１８に示すシーケンスに従って、図１に示す網5bに在圏するMN4の認証及び位置登録のシーケンスを説明する。本実施例において、MN4は、識別子と秘密鍵と公開鍵を、Secure Multimedia Card（SMMC）等の記憶装置から読み出す手段を備える。また、MN4は、DHCP-PD Requesting Router機能を備えるとする。

【００３５】

電源を入れたMN4は、網5bに属するルータ6cからルータ広告（Router Avertisement）を受信する(101)。MN4はRouter AvertisementのMビットを参照して、CoA（Care of Address）の取得方法を決定する。Mビットが１であれば、MNはIPv6ステートフルアドレス自動構成を用いてCoAを取得する。Mビットが設定されていなければ、MNはIPv6ステートレスアドレス自動構成を用いてCoAを生成する(102)。

【００３６】

次に、MN4は、ルータ6cに機器認証要求を送信する(103)。ルータ6cは、機器IDを検索キーとして機器認証を行う。ルータ6cは、MN4に対して認証結果を含む機器認証応答を送信する(104)。機器IDとして、例えばMACアドレスを用いる。

【００３７】

機器認証が正常に終了すると、MN4は、SMMC等の記憶装置からMN4の識別子と秘密鍵と公開鍵を読み出す。MN4の識別子は、例えばFQDN(Fully Qualified Domain Name)やX.500のDistinguished Nameで指定する。

【００３８】

MN４は、CA3に対しMN4の公開鍵と識別子を含む公開鍵証明書発行要求を送信する(105)。公開鍵証明書の送受信には、例えば、CMP (Certificate Management Protocol) を用いる。

【００３９】

図１１は、CMPメッセージを含むパケットのフォーマット例S1を示す。

【００４０】

図１０は、IPv6パケットのフォーマットを示す。

CMPメッセージS1は、IPv6パケットのPayload43内のデータ部43Bに格納される。

【００４１】

CA3は、上記要求を受信し、公開鍵証明書発行ルーチン80を起動する。

【００４２】

図９は公開鍵証明書発行ルーチン80を示す。CA3は、MN4の識別子を用いてMN4に証明書を発行可能であるか確認し（81）、発行可能であれば、MN4の公開鍵証明書を発行する。次に、CA3はPrefix配布管理テーブル330にMN4の新規エントリを生成し、Prefix発行許可フラグを設定する(82、106)。CA3は、MN4に対してMN4の公開鍵証明書とCA3の公開鍵を含む公開鍵発行要求応答を送信し、本ルーチンを終了する(83、107)。

ステップ81において証明書の発行が不可能でなる場合、或いは、ステップ82においてMN4の公開鍵に対して証明書を発行できない場合、CA3はMN4に対してエラーを通知する証明書発行要求応答を送信し(84)、本ルーチンを終了する。

HA１のサーバ部11はMN４と同様に識別子と秘密鍵と公開鍵を保持する。サーバ部11は、CA3からサーバ部11の公開鍵証明書を取得する。

MN4は、公開鍵証明書を取得すると、Prefix Request処理を起動し、ホームPrefixを取得する。

MN4は、Prefixの配布が可能なDHCP Serverを発見するため、DHCP Solicitメッセ

ージをAll_DHCP_Relay_Agents_and_Servers address宛に送信する（108）。上記Solicitメッセージは DHCP Clinet識別子(Client Identifier option)とIA_PD optionsを含む。上記IA_PD optionsには、Prefixを付与するグループ（IA_PD）をMN内で一意に示すIAIDが設定される。

【００４３】

図１２は、DHCPv6メッセージを含むパケットフォーマット例S2を示す。DHCPv6はトランスポートレイヤにUDP/IPを使うアプリケーションプロトコルである。DHCPメッセージS2は、IPv6パケットのPayload43内のデータ部43Bに格納される。DHCPメッセージは、Message-typeフィールド51の値で指定する。DHCPメッセージのオプションパラメータは、Optionsフィールド53に設定される。
ここで、HA１のサーバ部12が上記DHCP Solicitメッセージ（108）を受信したとする。HA1のサーバ部12は、Prefix Delegation処理ルーチン60を起動する。

【００４４】

図５は、Prefix Delegation処理ルーチン60を示す。

【００４５】

サーバ部12は、上記DHCP SolicitメッセージのIA_PD optionsからIAIDを読み出し、IAIDに対してPrefixを配布可能であるか判断する(61)。配布可能であれば、サーバ部12は、上記DHCP Solicitに含まれるIAIDからIA_PDを特定する。サーバ部12は、IA_PD を検索キーとして、IA_PDとMN4の識別子の対応テーブルを参照し、MN４の識別子を決定する。サーバ部12は、CA3にMN4の識別子を含む問合せを送信する(62、109)。

【００４６】

CA3は、上記問い合わせを受信すると、NN4の識別子を検索キーとしてPrefix配布管理テーブル330を検索する(110)。

【００４７】

CA3は、ステップ106で生成したMN4のエントリを検出する。CA3は該当エントリのPrefix発行許可フラグが設定されていることを確認して、サーバ部12にPrefix割当許可を示す応答を送信する（63、111）。

【００４８】

サーバ部12は、上記応答を受信すると、上記DHCP Solicitメッセージに含まれるDHCP Clinet識別子とIAIDでPrefix管理テーブル320を検索する。該当エントリがPrefix管理テーブル320に存在しなければ、サーバ部12はPrefix管理テーブル320に新規エントリを生成し、上記DHCP Solicitメッセージに含まれるDHCP Clinet識別子321とIAID322を格納する。そして、サーバ部12はMN4にDHCP Advertiseメッセージを送信する（64、112）。上記Advertiseメッセージは、サーバ部12の識別子(Server Identifier option)と、上記MN4の識別子(Client Identifier option)と、ステップ108で受信したIA_PD optionsを含む。サーバ部12は、DHCP Advertiseメッセージに配布可能なIPv6 Prefix情報を含んでもよい。

ステップ61において、サーバ部12がIAIDに対してIPv6 Prefixを配布することができないとき、或いは、ステップ63において、CA3がPrefixの配布を許可しないとき、サーバ部12は上記MN4にPrefix配布不可を示すStatus Code optionを含むAdvertiseメッセージを送信し、本ルーチンを終了する（67）。

【００４９】

MN4は、Prefixの配布が許可された場合、上記サーバ部12にIA_PD options を含むDHCP Requestメッセージを送信し、IPv6 Prefix情報を要求する（113）。

ステップ112で受信したAdvertiseメッセージがIPv6 Prefix情報を含む場合、上記Requestメッセージは、MN4が利用を希望するPrefixを含む。

ここで、図5に戻りPrefix Delegation処理ルーチン60の説明を続ける。

サーバ部12は、上記DHCP Reqeustメッセージを受信すると（65）、IAIDを読み出し、配布するIPv6 Prefixを特定する。上記RequestメッセージがIPv6 Prefix情報を含む場合、MN4が利用を希望するPrefixを承認する。

次に、サーバ部12は、上記DHCP Reqeustメッセージに含まれるDHCP Clinet識別子とIAIDでPrefix管理テーブル320を検索する。サーバ部12は、ステップ64で生成したエントリを検出して、該当エントリに配布するIPv6 PrefixとPrefixのライフタイムを格納する。サーバ部12はMN4に対してPrefix情報を含むDHCP Replyメッセージを送信して（66、114）、本ルーチンを終了する。

ステップ65においてMN4に配布するPrefixが特定できなかった場合、或いは、ステップ66においてPrefix管理テーブル320に該当エントリが存在しない場合、上

記サーバ部12はMN4にエラーを通知するDHCP Replyメッセージを送信し(68)、本ルーチンを終了する。

MN4は、上記DHCP Replyメッセージから IPv6 Prefix情報を抽出する。MN4は上記Prefix情報とMN4のインタフェース識別子からホームアドレスを生成する（115）。

【００５０】

次にMN4は、HAアドレス発見機能を用いてHAアドレスを特定する。MN4は、ステップ114で受信したPrefixをホーム網のPrefixに設定したMobile IPv6 Home-Agents Anycast Address宛に、HAアドレス発見要求（Home Agent Address Discovery Request）を送信する(116)。

上記Mobile IPv6 Home-Agents Anycast Addressと同一Prefixを有するHAのいずれかが上記Home Agent Address Discovery Requestを受信する。

ここで、HA１のサーバ部11aが、上記Home Agent Address Discovery Requestを受信したとする。サーバ部11aは、MN4にHAアドレス発見応答（Home Agent Address Discovery Reply）を送信する(117)。

【００５１】

MN4は、上記Home Agent Address Discovery Replyを受信して、HAアドレス（サーバ部11aのアドレス）を取得する（118）。

次に、MN4は、IKEを用いてMN4とサーバ部11aとの間にIPsec SAを生成する。

IKEフェーズ１において、MN4とサーバ部11aの間にISAKMP SAを確立する。ISAKMP SAはIKEの制御用チャネルである

MN4は、サーバ部11aに、SAペイロードを用いてISAKMP SAのパラメータを提案する（121）。

【００５２】

図１３は、ISAKMPのパケットフォーマット例S3を示す。IKEで使用するパケットのフォーマットは、ISAKMPプロトコルで規定される。IKEのトランスポートプロトコルはUDP/IPである。

ISAKMPパケットS3は、IPv6パケットのPayload43内のデータ部43Bに格納される。

ISAKMPパケットS3は、ISAKMPヘッダ55と１つ以上のペイロード56で構成される。

ペイロード56には、例えば、SAの提案を運ぶSAペイロード、ID情報を交換するIdentificationペイロード、デジタル署名を送信するSignitureペイロードなどがある。

サーバ部11aは、ステップ121で受信したSAペイロードから受諾可能なProposalを選択してMN4に返信する（122）。

次に、MN4とサーバ部11aは、Diffe-Hellman公開値とNonceによる乱数を交換して（123、124）、秘密対称鍵を生成する。

続いて、MN4とサーバ部11aは、本人性を確認するため、ID情報を交換する。なお、本実施例では、本人であるかどうかの属性の確認の際に伝送される信号を本人性確認信号と定義している。図14は、IKEフェーズ１の本人性確認に用いるISAKMPパケットのフォーマット例S4を示す。ISAKMPパケットS4は、 Identificationペイロード56AとSignitureペイロード56Ｂ、Certificateペイロード56Cを含む。

MN4は、サーバ部11aに本人性確認に用いるISAKMPパケットを送信する(125)。上記ISAKMPパケット125のIdentificationペイロード56Aは、MN4がステップ115で生成したホームアドレスを含む。MN4は、ハッシュ値を計算し、そのハッシュ値にMN4の秘密鍵を用いてデジタル署名を行い、Signitureペイロード56Bに設定する。Certificateペイロード56Cは、CA3が発行したMN4の公開鍵証明書を含む。

サーバ部11aは、上記パケット125のSignitureペイロード56BからMN4のデジタル署名を取り出し、MN4の公開鍵を使ってデジタル署名を復号化する。MN4の公開鍵は、上記パケット125のCertificateペイロード56Cから取得する。

受信パケット125から計算したハッシュ値と、上記デジタル署名を復号化した値を比較することにより、サーバ部11ａはパケット送信者MN4の本人性を確認する。

次にサーバ部11aは、上記パケット125のIdentificationペイロードからMN4のホームアドレスを取り出す。サーバ部11aは、サーバ部12にホームプレフィックスを含む問い合わせを送信する（126）。サーバ部12は、上記問合せ126に含まれるPrefixを検索キーとして、Prefix管理テーブル320を検索する。上記Prefix管理テーブル320に該当エントリが存在すれば、Prefixは割当済みである（127）。サーバ部12は、サーバ部11aに対してPrefix割当済みを通知する応答を送信する（1

28）。

Prefixが割当済みであれば、サーバ部11aは、IKEフェーズ１の処理を継続する。サーバ部11aはハッシュ値にサーバ部11aの公開鍵を使ってデジタル署名を行う。サーバ部11aは、MN4に上記デジタル署名を含むISAKMPパケットを送信する（129）。上記ISAKMPパケット129のIdentificationペイロードには、サーバ部11aのIPアドレスを設定する。上記ISAKMPパケットはサーバ部11aの公開鍵証明書を含んでもよい。

MN4は、上記パケット129を受信し、サーバ部11aの公開鍵を使ってIKE通信相手が本物であることを確認する。MN4は、サーバ部11aの公開鍵を上記パケット129の公開鍵証明書、或いは、CA3から取得する。

以上で、MN4とサーバ部11aの間にISAKMP SAが確立する。

次に、IKEフェーズ2において、MN4とサーバ部11a間にIPsec SAを生成する。上記IPsec SAは、MN4とサーバ部11aとの間のパケットをIPsec化して転送する際に利用する。IKEフェーズ2で送受信されるISAKMPパケットのペイロードは、IKEフェーズ1で確立したISAKMP SAによって暗号化される。

MN4は、サーバ部11aにIPsec SAプロポーザルを含むSAペイロードと、Nonceペイロードと、ハッシュペイロードを設定したISAKMPパケットを送信する（130）。

サーバ部11aは、MN4に、受諾したIPsec SAのプロポーザルを含むSAペイロードと、Nonceペイロードと、ハッシュペイロードを設定したISAKMPパケットを送信する（131）。

MN4はサーバ部11aにハッシュペイロードを含むISAKMPパケットを送信する（132）。サーバ部11aは、上記パケット132を受信して、NN4が上記パケット131を受信したことを確認する。以上の処理により、２本のIPsec SA(MN4からサーバ部11aへのIPsec SAとサーバ部11aからMN4へのIPsec SA)が生成される。サーバ部11aとMN4は、上記IPsec SA（SPI、MN4のホームアドレス、サーバ部11aのアドレス等）をそれぞれSADに格納する。

MN4は、サーバ部11aに、上記IKEフェーズ2で生成したSAを適用した位置登録メッセージ（Binidng Update）を送信する（133）。MN4は、Binding Update List管理テーブルにサーバ部11aのアドレスを仮登録する（134）。

【００５３】

図１５は、IPsecを適用したBinding Updateのメッセージフォーマット例S11を示す。IPv6 Destination Options Header401と、IPsecヘッダ（AH HeaderまたはESP Header）402と、IPv6 Mobility Header403は、IPv6パケットの拡張ヘッダ42に格納される。

MN4がサーバ部11aに送信するBinding Updateには、以下の値が格納される。MN4のCoAがIPv6パケットヘッダの送信元アドレス41aに設定される。MN4がステップ115で生成したホームアドレスがIPv6 Destination Options Header401のHome Addresフィールドに設定される。

サーバ部11aは、上記Binding Update133を受信し、IPsec処理ルーチン70を起動する。

【００５４】

図６は、IPsec処理ルーチン70を示す。まず、IPv6 Destination Options Header401を処理する（71）。具体的には、Destination Options Headerの値（ホームアドレス）と送信元アドレスの値（CoA）を入れ替える。

【００５５】

次に、サーバ部11aは、SADをIPsecの種類（AH or ESP）、SPI値、及び、着信先アドレスで検索し、IPsec SAを特定する。受信パケットが暗号化されている場合、サーバ部11aは受信パケットを復号化した後、特定したIPsec SAに合致することを確認する（72）。次にサーバ部11aは、SPDを参照して、再構築したパケットが受け入れ可能であるかチェックする（73）。

パケットを受け入れ可能であれば、サーバ部11aのIPsec処理部14は上記再構築されたパケットをMobile IP処理部15に送信する。

【００５６】

Mobile IP処理部15は、MN4の位置登録処理を行う（74）。

Mobile IP処理部15は、MN4のホームアドレスを検索キーとして、Binding Cache管理テーブル310を検索する。上記Binding Cache管理テーブル310にMN4のエントリが存在しなければ、上記Binding Cache管理テーブル310にMN4のエントリを追加する（135）。上記エントリのCare of Address312には、MN4が在圏網5bで取得

したCoAを設定する。

ステップ72及びステップ73において処理が正常に終了しなかった場合、サーバ部11aは受信パケットを廃棄し、本ルーチンを終了する（78）。

【００５７】

Mobile IP処理部15は、MN4に対してIPsecを適用したBinding Updateの応答（Binding Acknowledgement）を送信するため、IPsec処理部14にパケットを送信する。IPsec処理部14は、SPDを検索して上記パケットのセキュリティポリシーを調べる（75）。上記パケットはIPsecの適用対象であることがわかり、SADから合致するSAを検出する。IPsec処理部14は、上記パケットにRouteing Header404を追加し、IPsecを適用する（76）。次にサーバ部11aは、Routeing Headerの値と着信先アドレスの値を入れ替え、MN4にIPsecを適用したBinding Acknowlegementを送信し（77、136）、本ルーチンを終了する。

【００５８】

図１６は、IPsecを適用したBinding Acknowledgementメッセージのフォーマット例S12を示す。IPv6 Routing Header404と、IPsecヘッダ（AH Header or ESP Header）402と、IPv6 Mobility Header403は、IPv6パケットの拡張ヘッダ42に格納される。サーバ部11aがMN4に送信するBinding Acknowledgementには、以下の値が格納される。MN4のCoAがIPv6パケットヘッダの着信先アドレス41bに格納される。MN4のホームアドレスがIPv6 Routing Header404のHome Addressフィールドに格納される。

【００５９】

MN4は、Binidng Acknowledgement136を受信すると、SADを検索してSAを特定する。受信パケットが暗号化されている場合、復号化した後SAに合致することを確認する。さらにSPDを参照して、再構築したパケットが受け入れ可能であるかチェックする。受け入れ可能であれば、MN4はステップ134で仮登録したエントリをBinding Update List管理テーブルに登録する（137）。

【００６０】

ここで、MN4は識別情報（例えばFQDN）とステップ115で取得したホームアドレスの対応情報をホーム網8、在圏網５、或いは、IP網７に属する位置情報管理装

置（例えばDNSサーバ装置）に登録してもよい。

【００６１】

情報家電端末9がMobile IPv6機能とDHCP-PD Requesting Router機能を備え、CA3から公開鍵証明書を取得すれば、上記認証方法を情報家電端末9に適用できる。

本発明の第１の実施の形態によると、デジタル署名認証方法とMobile IPの位置登録手順が連携し、HAが公開鍵証明書にリンクしたホームアドレスに対してSAを生成・保持することにより、IPv6端末の正当性を確認する認証方法の提供が可能になる。

【００６２】

MN4とHA１のサーバ部11はCA3が発行した公開鍵証明書を保持し、HA１のサーバ部12とMN4がDHCP-PD機能を備える。CA3とHA１のサーバ部12の連携により、HA１はCA3がPrefixの配布を許可したMN4に対してPrefixの通知が可能になる。さらに、HA１のサーバ部11は、サーバ部12が割り当てたPrefixをホームプレフィックスとするMN4との間でIPsec SAを生成することにより、MNの正当性を確認する認証方法の提供が可能になる。

（実施例２）

本発明の第2の実施の形態を図面を用いて説明する。

【００６３】

図１９は、本発明の第2の実施例における通信網の構成例を示す。第2の実施例は、通信装置2がDHCP-PD Requesting Router機能を備えることを特徴とする。第2の実施例において、IP網7は認証サーバ10を備える。認証サーバ10はホーム網へのアクセス認証に必要な情報（ID、パスワード等）を管理する。

【００６４】

図２０は、本発明の第2の実施例における通信装置2の構成例を示す。通信装置2はCPU21と、メモリ22と、回線24（24a、24b）を収容するインタフェース部（IF）23（23a、23b）とを、バス25で接続する構成をとる。

【００６５】

メモリ22は、主にDHCP-PD Requesting Router機能を備えるDHCP PD機能部26と

、ホーム網8へのアクセス認証を行う認証処理部27とを備える。

【００６６】

図２１は、本発明の第2の実施例におけるMN4の認証及び位置登録のシーケンスを示す。

第1の実施例と第2の実施例は、DHCP-PD Requesting Router機能の配備箇所が異なる。第2の実施例において通信装置2（GW2）がDHCP-PD Requesting Router機能を備え、DHCP-PDメッセージを送受信する。

ステップ101からステップ107は、第1の実施例と同様である。

以下、ステップ141以降について説明する。

GW2は、MN4からパケットを受信すると、MN4に対して認証情報を要求する（141）。MN4は、IDとパスワードを含む認証要求を送信する（142）。GW2bはIAIDを含むDHCP Solicitを送信する（143）。

サーバ部12は、上記DHCP Solicit受信し、IAIDからIA_PDを特定する。サーバ部12は、IA_PD を検索キーとして、IA_PDとMN4の識別子の対応テーブルを参照し、ＭＮ４の識別子を決定する。

ステップ144からステップ146は、第１の実施例におけるステップ109からステップ111と同様である。

【００６７】

サーバ部12は、応答146を受信すると、GW2bにDHCP Advertiseを送信する（147）。以下、サーバ部12におけるステップ148とステップ149の処理は、第1の実施例と同様である。

【００６８】

GW2bは、Prefix情報を含むDHCP Solicit149を受信すると、MN4にPrefix情報を含む認証応答を送信する（150）。以下、MNの認証処理及び位置登録処理は、第1の実施例のステップ115からステップ137と同様である。

本発明の第2の実施の形態によると、通信装置2がDHCP-PD Requesting Router機能を備える場合であっても、デジタル署名認証方法とMobile IPの位置登録手順の連携により、DHCP-PD機能を備えないIPv6端末の正当性を確認する認証方法が提供できる。

また、上記通信装置2がHAへのアクセス認証機能を提供することにより、より安全性の高い通信サービスの提供が可能になる。

（実施例３）

本発明の第3の実施の形態を図面を用いて説明する。

【００６９】

図２２は、本発明の第3の実施例における通信網の構成例を示す。第3の実施例は、第2の実施例に示す機能に加えて、通信装置2がHMIPv6のMAP機能を備えることを特徴とする。第3の実施例において、MN4はHMIPv6対応移動端末である。

【００７０】

図２３は、第3の実施例における通信装置2の構成例を示す。通信装置2のメモリ22は、第2の実施例に示す機能に加えてHMIPv6処理部29を備える。HMIPv6処理部29はHMIPv6のMAP機能を提供し、RCoAとLCoAの対応情報を保持するBinding Cache管理テーブルを備える。

【００７１】

図２４に示すシーケンスに従って、図22に示す網5bに在圏するMN4の認証及び位置登録のシーケンスを説明する。

【００７２】

MN4は網5bに属するルータ（AR：Access Router）6cからMAPオプションを含むルータ広告（Router Avertisement）を受信する(161)。MN4は、ルータ広告161の情報を用いて、通信装置（以下、MAP）2bを特定し、RCoAとLCoAを生成する(162)。

【００７３】

ステップ103からステップ107は、第1の実施例と同様である。

【００７４】

MN4は、CA3から公開鍵証明書を受信すると、 MAP2bに位置登録信号（Binding Update）を送信する(163)。

【００７５】

第3の実施例において、MAP2bは位置登録信号の受信を契機に認証処理を起動する。以下、ステップ141からステップ150は、第2の実施例と同様である。

【００７６】

ステップ150までの処理が正常に終了した場合、MAP2bはHMIPv6処理部29のBinding Cache管理テーブルにMN4のRCoAとLCoAの対応情報を格納する。MAP2bはMN4にBinidng Acknowledgementを送信する（164）。

【００７７】

以下、MNの認証処理及び位置登録処理は、第1の実施例のステップ115からステップ137と同様である。

本発明の第3の実施例によると、通信装置2がHMIPv6機能を備える場合であっても、デジタル署名認証方法とMobile IPの位置登録手順の連携により、DHCP-PD機能を備えないIPv6端末の正当性を確認する認証方法が提供できる。

また、上記通信装置はHMIPv6の制御信号受信を契機に、ホーム網に対するアクセス認証処理を起動することが可能になり、より安全性の高い通信サービスの提供が可能になる。

（実施例４）

本発明の第4の実施の形態を図面を用いて説明する。本発明の第4の実施例における通信網の構成例は、第1の実施と同様である。

【００７８】

第4の実施例は、HA１のサーバ部11が、CA3によって許可されたMNにしてPrefixを配布する手段と、ＭＮ4の公開鍵証明書管理テーブルを備えることを特徴とする。公開鍵証明書管理テーブルは、IPsecフェーズ１のISAKMPパケットに含まれるIdentificationペイロードの情報と公開鍵証明書の対応情報を格納する。

【００７９】

第4の実施例において、HA１とMNは、DHCP-PD機能を備えなくてもよい。MN4のHAは、サーバ部11ａとする。

【００８０】

図25から図27に示すシーケンスに従って、図１に示す網5bに在圏するMN4がHA1のサーバ部11aに位置登録を完了後、HA1のサーバ部11aがMN4にプレフィックスを通知し、MN4が再度位置登録を完了するまでのシーケンスを説明する。

ステップ101からステップ107は、第1の実施例と同様である。

続いて、MN4はサーバ部11aとの間でIPsec SAを生成する。

ステップ121からステップ125は、第1の実施例と同様である。MN4は、サーバ部11aに対して、 MN4のホームアドレスを設定したIdentificationペイロードとMN4の公開鍵証明書を設定したCertificateペイロードを含むISAKMPパケット125を送信する。

サーバ部11aは、上記パケット125からIdentificationペイロードとCertificateペイロードの情報を読み出し、MN4のエントリを公開鍵証明書管理テーブルに追加する（171）。MN4のエントリが存在する場合は、該当エントリを更新する。

ステップ129からステップ132は、第1の実施例と同様である。

MN4はサーバ部11aとの間に生成したIPsec SAを適用して位置登録を行う。位置登録処理（ステップ133から137）は、第1の実施例と同様である。

サーバ部11aは、例えば自身のPrefixを変更する場合、位置登録中のMN4に対してプレフィックスを通知する。

まず、サーバ部11aは、Binding Cache管理テーブル310を参照し、ステップ135で生成したMN4のエントリを検出する。次に、サーバ部11aは、MN4のホームアドレスを検索キーとして、公開鍵証明書管理テーブルを検索し、ステップ171で生成したMN4の公開鍵証明書を読み出す。

サーバ部11aはMN4の公開鍵証明書からＭＮ４の識別子を特定し、上記MN4の識別子を含む問合せをCA3に送信する（173）。

【００８１】

CA3は、上記問い合わせを受信すると、NN4の識別子を検索キーとしてPrefix配布管理テーブル330を検索する。

【００８２】

CA3は、ステップ106で生成したMN4のエントリを検出する。CA3は該当エントリのPrefix発行許可フラグが設定されていることを確認して（174）、サーバ部11aにPrefix割当許可を示す応答を送信する（175）。

【００８３】

サーバ部11aは、上記応答を受信すると、MN4にプレフィックス情報を通知するMobile Prefix Advertisementを送信する（176）。サーバ部11aは、上記Mobile

Prefix Advertisementメッセージに、ステップ130から132で生成したIPsec SAを適用する。

【００８４】

MN4は、上記Mobile Prefix Advertisementからプレフィックスを読み出す。MN4は、ホームプレフィックスの変更を検出し、ホームアドレスを生成する。ホームアドレスの生成から位置登録を完了するまでの処理（ステップ115～125、ステップ129～137）は、第1の実施例と同様である。

本発明の第4の実施例によると、HA1がCA3と連携することにより、MNの正当性を確認したのち、MN4にプレフィックス情報を通知することが可能になる。

【００８５】

【発明の効果】

以上の実施の形態から明らかなように、本発明はデジタル署名認証方法とMobile IPの位置登録手順の連携により、IPv6端末の正当性を確認する認証方法を提供する。

【００８６】

特に、領域Aに属するHAをホーム網とする端末ｘが領域BにおいてMobile IPの位置登録を行う際、領域Aに属するDHCP-PD Delegating Router機能が領域Bに属する端末XにPrefixを配布する手段を備え、１）DHCP-PD Delegating Router機能がCAにPrefix配布可否を問い合わせる手段、２）HAがDHCP-PD Delegating Router機能にPrefix情報を問い合わせる手段、３）HAが端末xとの間にIPsec SAを生成する際、端末xの公開鍵をCAまたは端末xから取得する手段、４）HAが上記3）で生成したIPsecを適用した位置登録のみ許容する手段、を備えることにより、端末ｘの正当性を確認する認証方法の提供が可能になる。

【００８７】

領域Aと領域Bを相互接続する通信装置がDHCP-PD Requesting Router機能と、領域Aへのアクセス認証機能を備えれば、 DHCP-PD機能を備えない端末xに対して上記認証方法の提供が可能になる。また、上記通信装置は認証された端末xのみHAへのアクセスを許容するため、安全性の高い通信サービスの提供が可能になる。

【００８８】

さらに、上記領域Aと領域Bを相互接続する通信装置が、HMIPv6のMAP機能を備えれば、上記通信装置はHMIPv6の制御信号受信を契機に、領域Aに対するアクセス認証処理を起動することが可能になる。

また、HA1がCA3との通信手段とMN4の公開鍵証明書を保持する手段を備えれば、HA1はCA3にMN4の正当性を確認したのち、MN4にプレフィックス情報を通知することが可能になる。

【図面の簡単な説明】

【図１】

本発明における通信網の構成例を示す構成図。

【図２】

HA１のブロック図。

【図３】

HA１が備えるBinding Cache管理テーブル図。

【図４】

HA１が備えるPrefix管理テーブル図。

【図５】

HA1のDHCP PD機能部が備えるPrefix Delegation処理ルーチン図。

【図６】

HA1のIPsec処理部が備えるIPsec処理ルーチン図。

【図７】

CA3のブロック図。

【図８】

CA3が備えるPrefix配布管理テーブル図。

【図９】

CA3が備える公開鍵証明書発行ルーチン図。

【図１０】

IPv6パケットのフォーマット図。

【図１１】

CMPメッセージ例の図。

【図１２】

DHCPv6パケットのフォーマット図。

【図１３】

ISAKMPパケットのフォーマット例の図。

【図１４】

IKEフェーズ１本人性確認時のISAKMPパケットのフォーマット例の図。

【図１５】

Binding Updateメッセージ例の図。

【図１６】

Binding Acknowledgementメッセージ例の図。

【図１７】

本発明における認証及び位置登録シーケンス図1。

【図１８】

本発明における認証及び位置登録シーケンス図2。

【図１９】

第2の実施例における通信網の構成例を示す構成図。

【図２０】

第2の実施例における通信装置2のブロック図。

【図２１】

第2の実施例における認証及び位置登録シーケンス図。

【図２２】

第3の実施例における通信網の構成例を示す構成図。

【図２３】

第3の実施例における通信装置2のブロック図。

【図２４】

第3の実施例における認証及び位置登録シーケンス図。

【図２５】

第4の実施例における認証及び位置登録シーケンス図1。

【図２６】

第4の実施例における認証及び位置登録シーケンス図2。

【図２７】

第4の実施例における認証及び位置登録シーケンス図3。

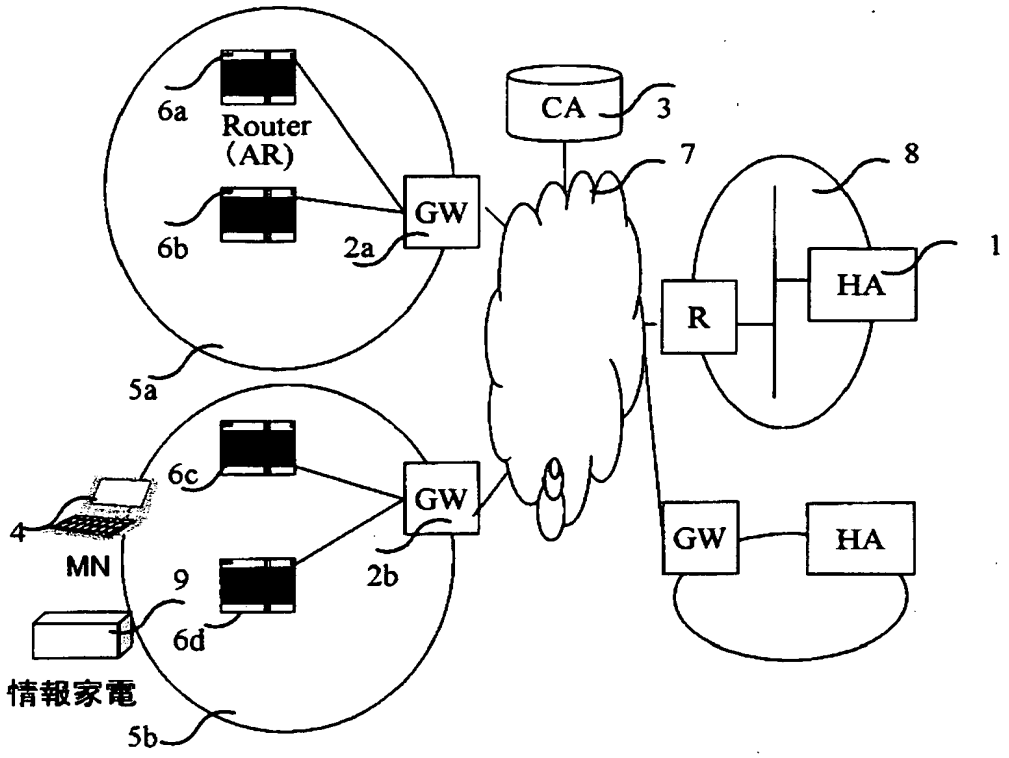
【符号の説明】

1 HA、2 通信装置、3 CA、4 Mobile IP移動ノード(MN)、60 Prefix Request処理ルーチン、70 IPsec処理ルーチン、80 証明書発行ルーチン。

【書類名】　図面

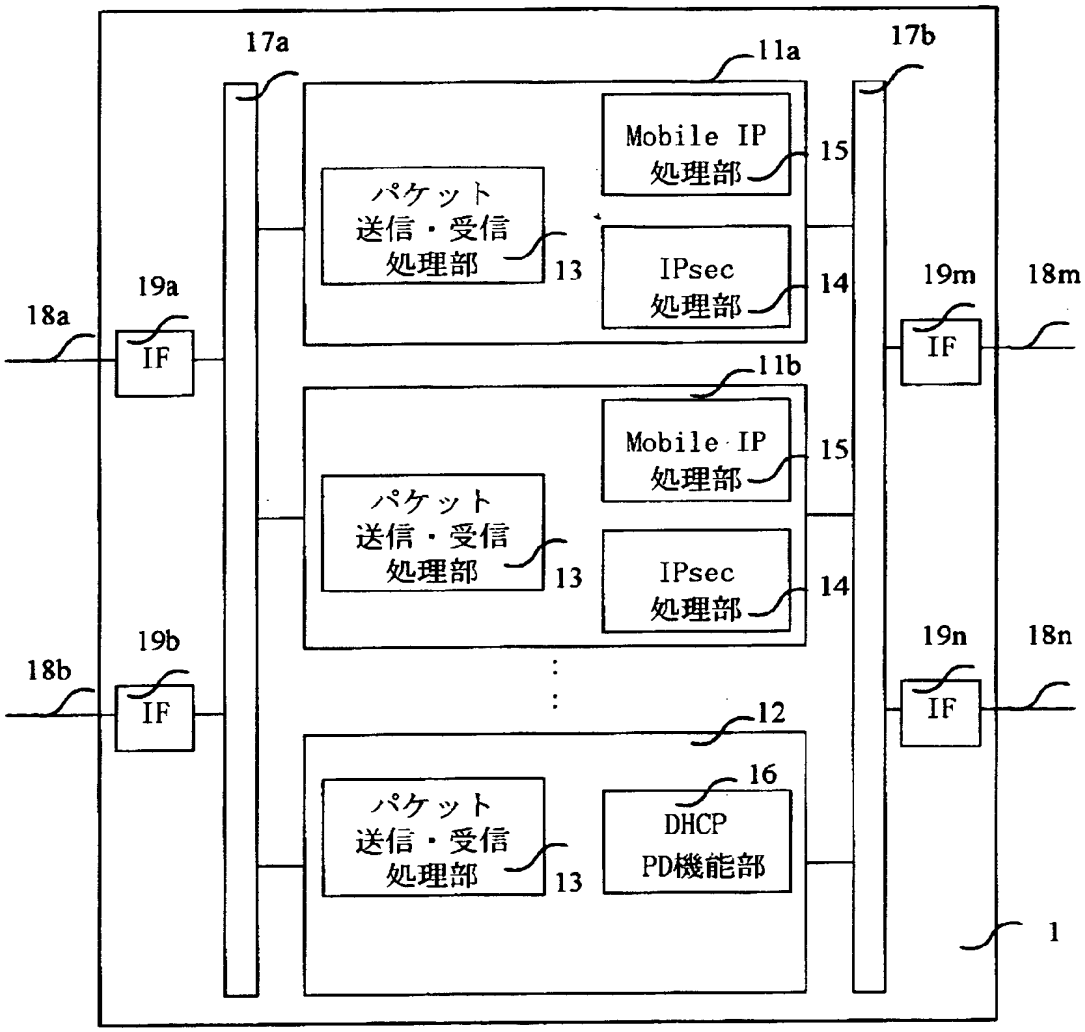
【図１】

図1



【図２】

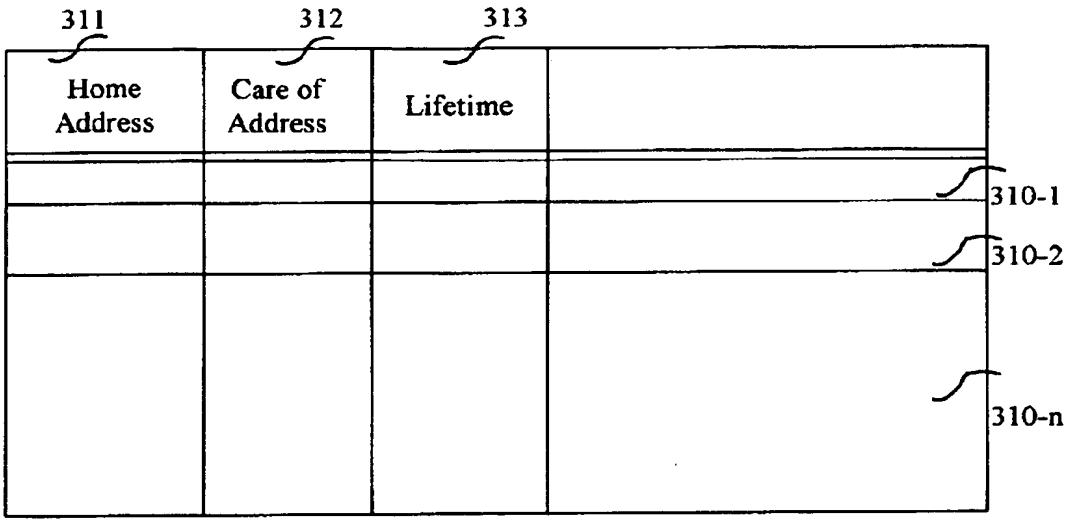
図2


17a
11a
17b
Mobile IP
処理部
15
パケット
送信・受信
処理部
13
IPsec
処理部
14
19a
18a
IF
19m
18m
IF
11b
Mobile IP
処理部
15
パケット
送信・受信
処理部
13
IPsec
処理部
14
19b
18b
IF
19n
18n
IF
12
16
パケット
送信・受信
処理部
13
DHCP
PD機能部
1

【図３】

図3

310　Binding Cache管理テーブル



【図４】

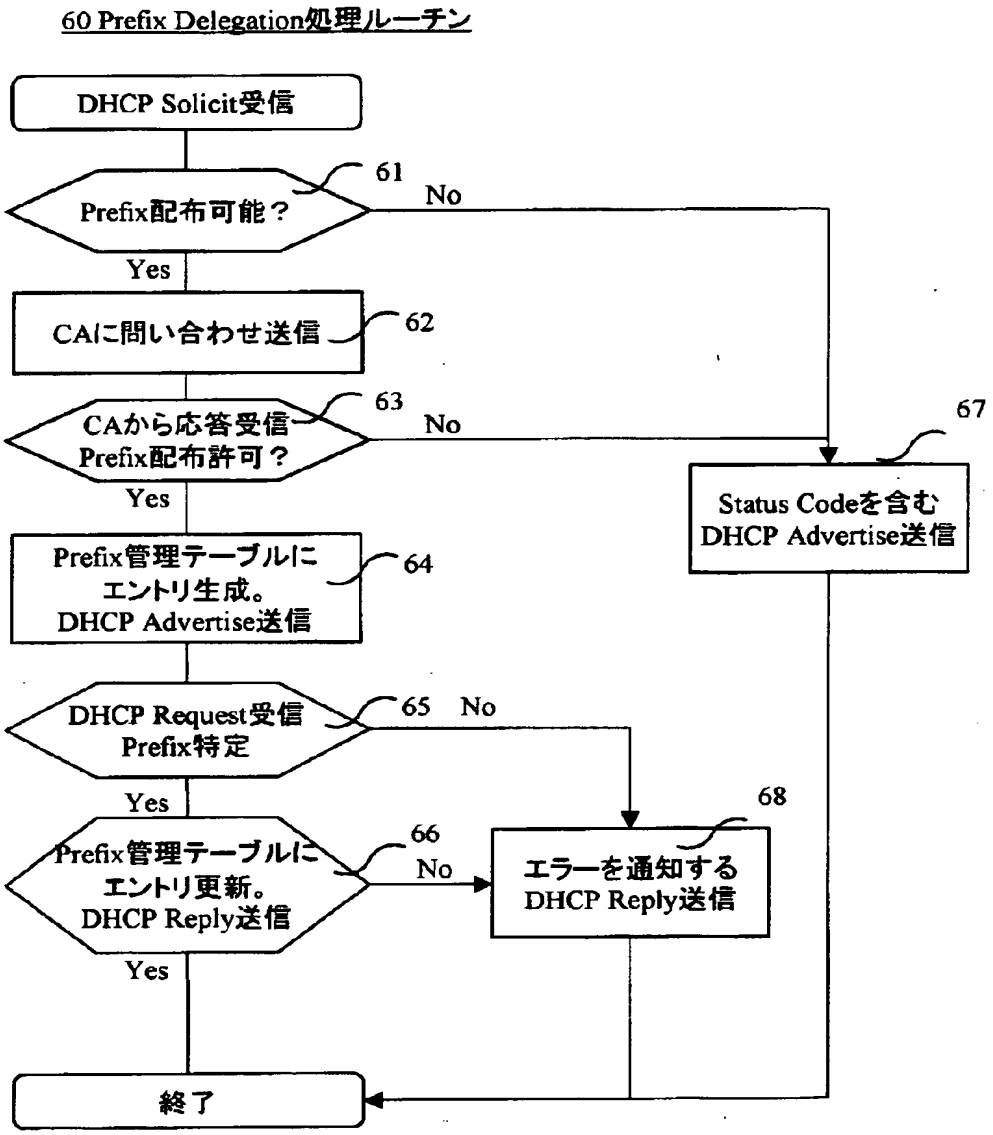
図4

320　Prefix 管理テーブル

321 DHCP Client 識別子	322 IAID	323 Prefix	324 Lifetime	
				320-1
				320-2
				320-n

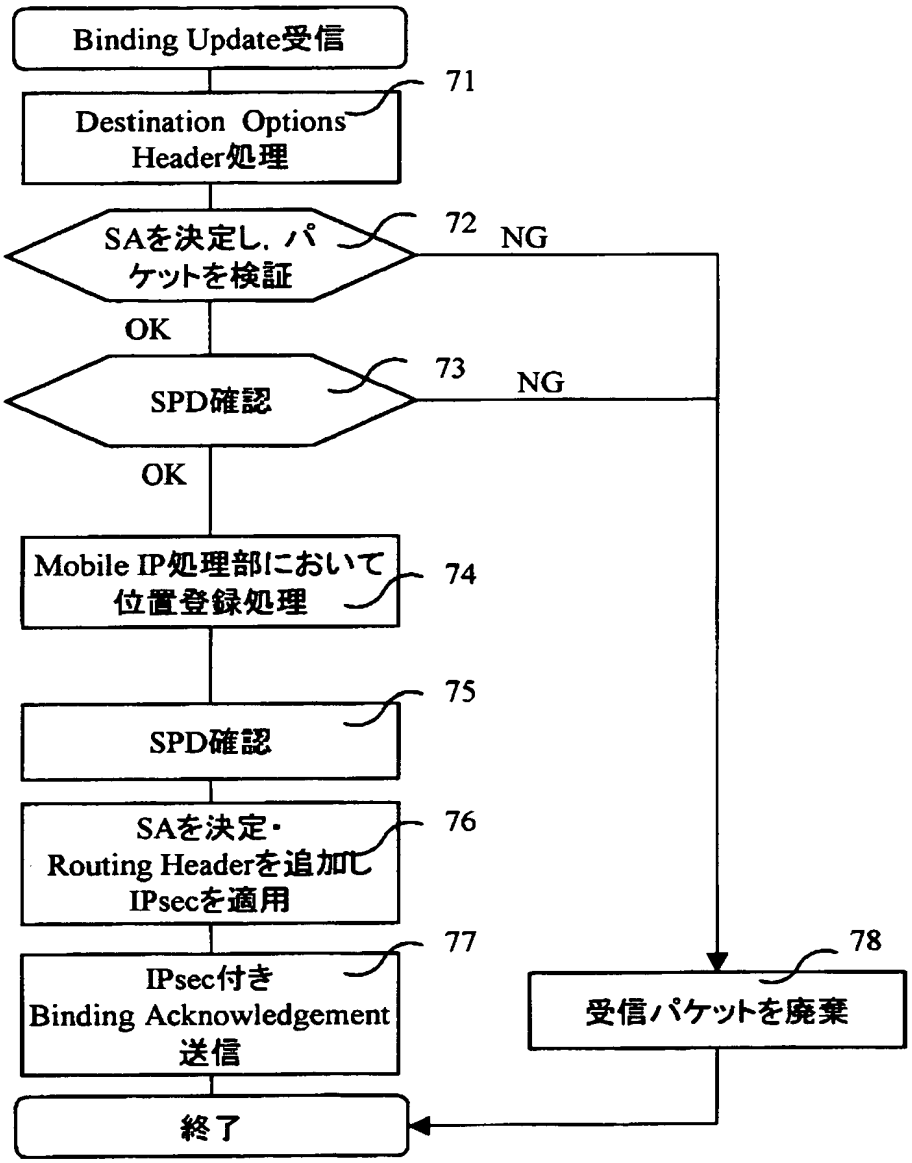
【図５】

図5


60 Prefix Delegation処理ルーチン
DHCP Solicit受信
61
Prefix配布可能？
No
Yes
CAに問い合わせ送信
62
CAから応答受信
Prefix配布許可？
63
No
67
Yes
Status Codeを含む
DHCP Advertise送信
Prefix管理テーブルに
エントリ生成。
DHCP Advertise送信
64
DHCP Request受信
Prefix特定
65
No
Yes
68
Prefix管理テーブルに
エントリ更新。
DHCP Reply送信
66
No
エラーを通知する
DHCP Reply送信
Yes
終了

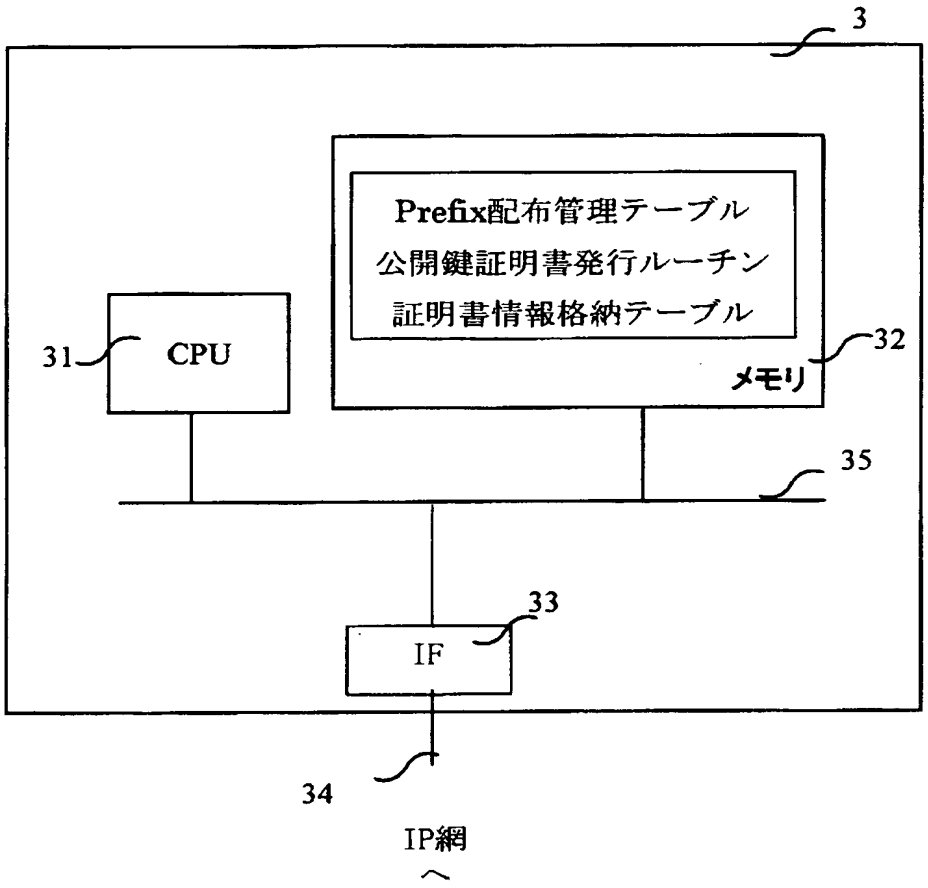
【図６】

図6


70 IPsec処理ルーチン
Binding Update受信
71
Destination Options Header処理
72
SAを決定し，パケットを検証
NG
OK
73
SPD確認
NG
OK
Mobile IP処理部において位置登録処理
74
75
SPD確認
SAを決定・Routing Headerを追加しIPsecを適用
76
77
IPsec付きBinding Acknowledgement送信
78
受信パケットを廃棄
終了

【図７】

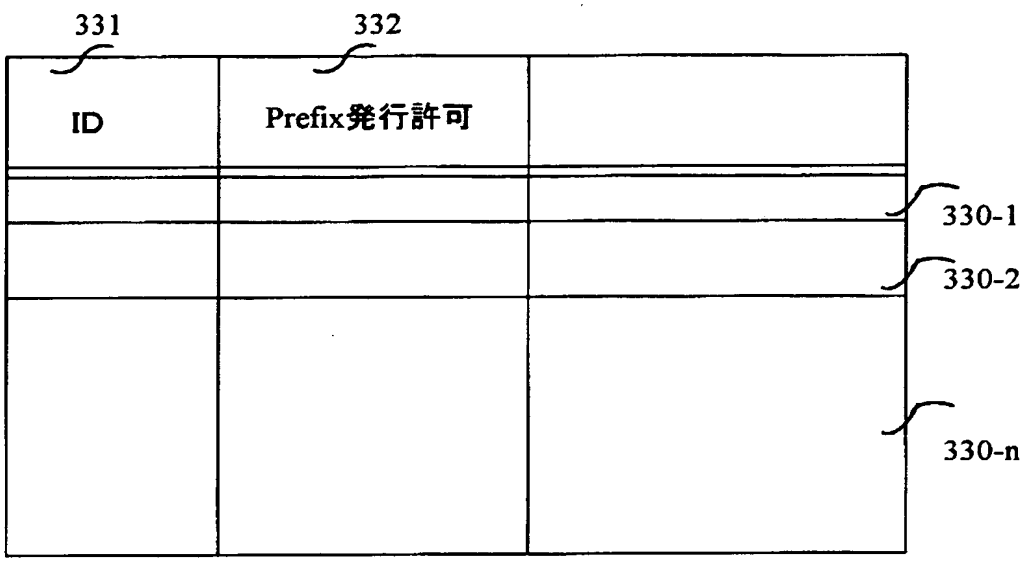
図7


3
Prefix配布管理テーブル
公開鍵証明書発行ルーチン
証明書情報格納テーブル
31
CPU
32
メモリ
35
33
IF
34
IP網
へ

【図８】

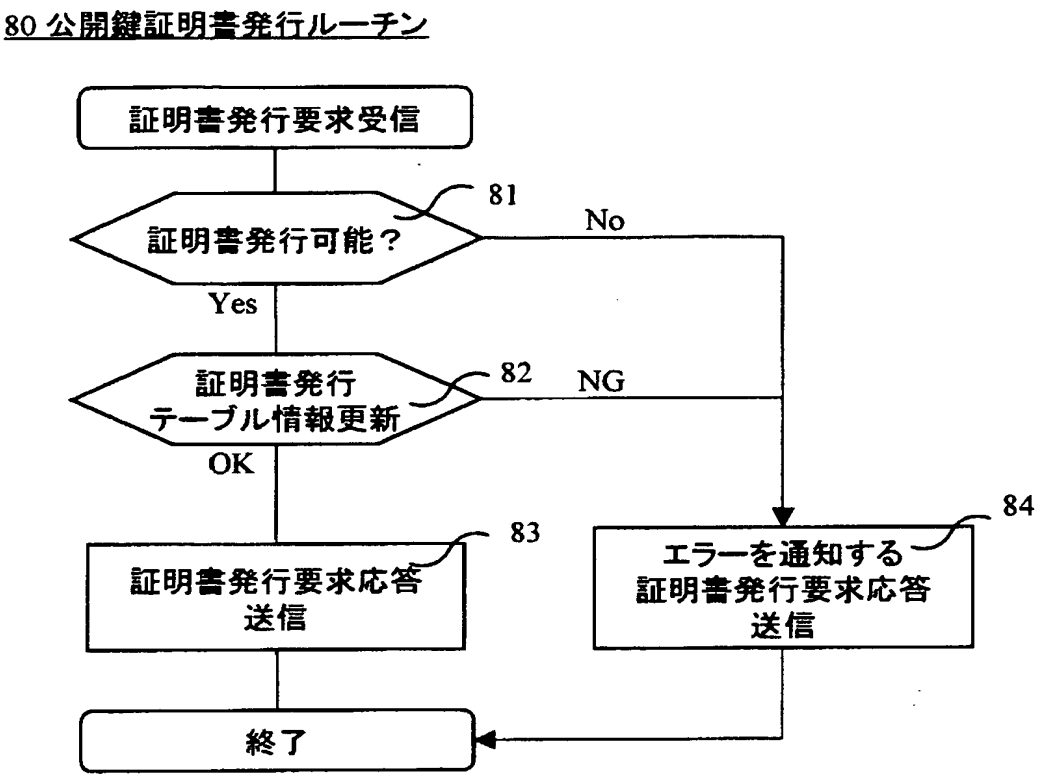
図8

330　Prefix配布管理テーブル(CA)



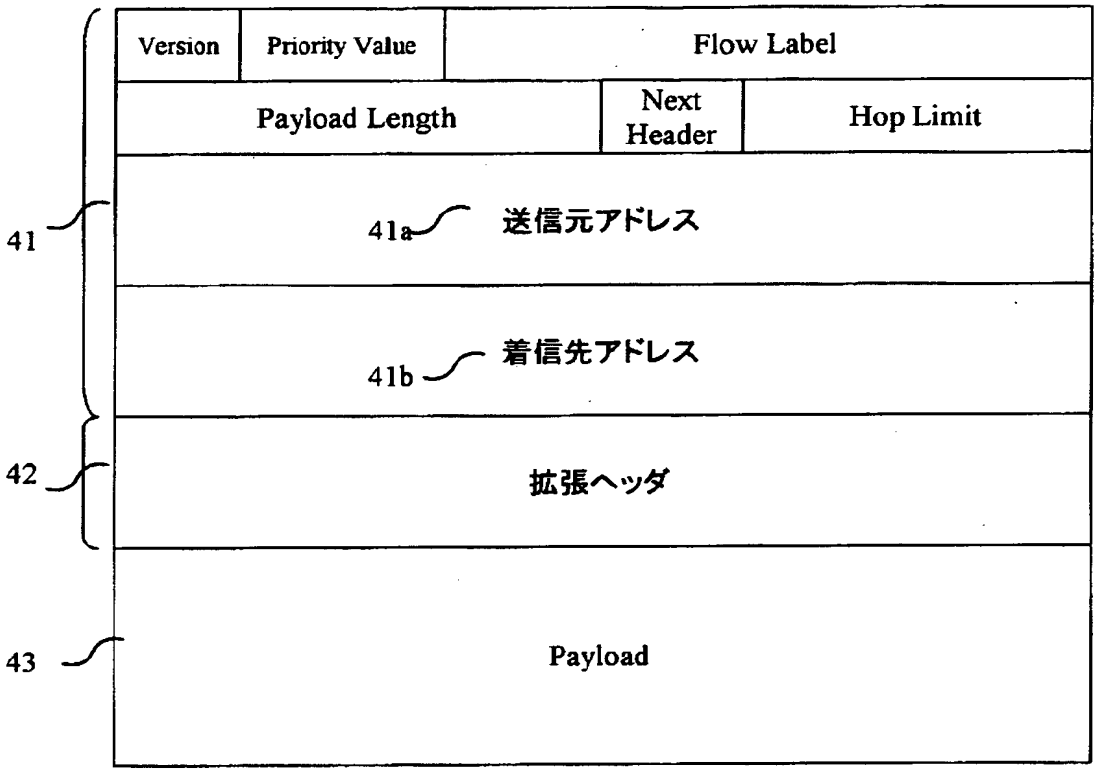
【図９】

図9


80 公開鍵証明書発行ルーチン
証明書発行要求受信
81
証明書発行可能？
No
Yes
証明書発行
テーブル情報更新
82
NG
OK
83
証明書発行要求応答
送信
84
エラーを通知する
証明書発行要求応答
送信
終了

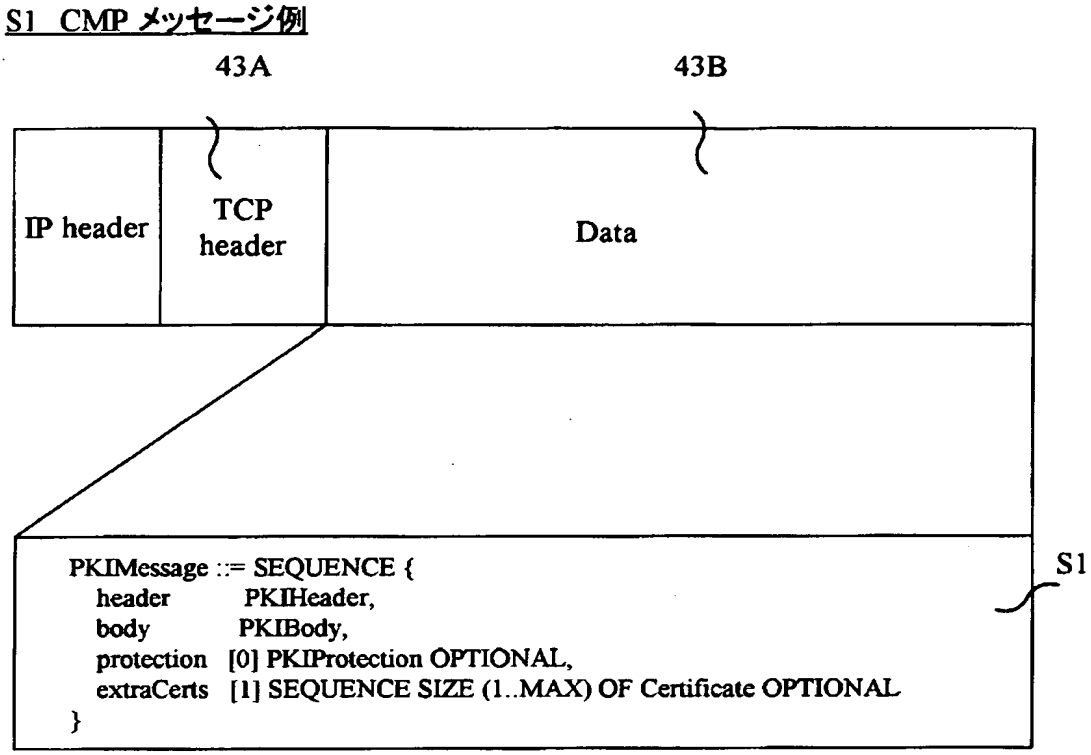
【図１０】

図10


Version
Priority Value
Flow Label
Payload Length
Next Header
Hop Limit
41
41a
送信元アドレス
41b
着信先アドレス
42
拡張ヘッダ
43
Payload

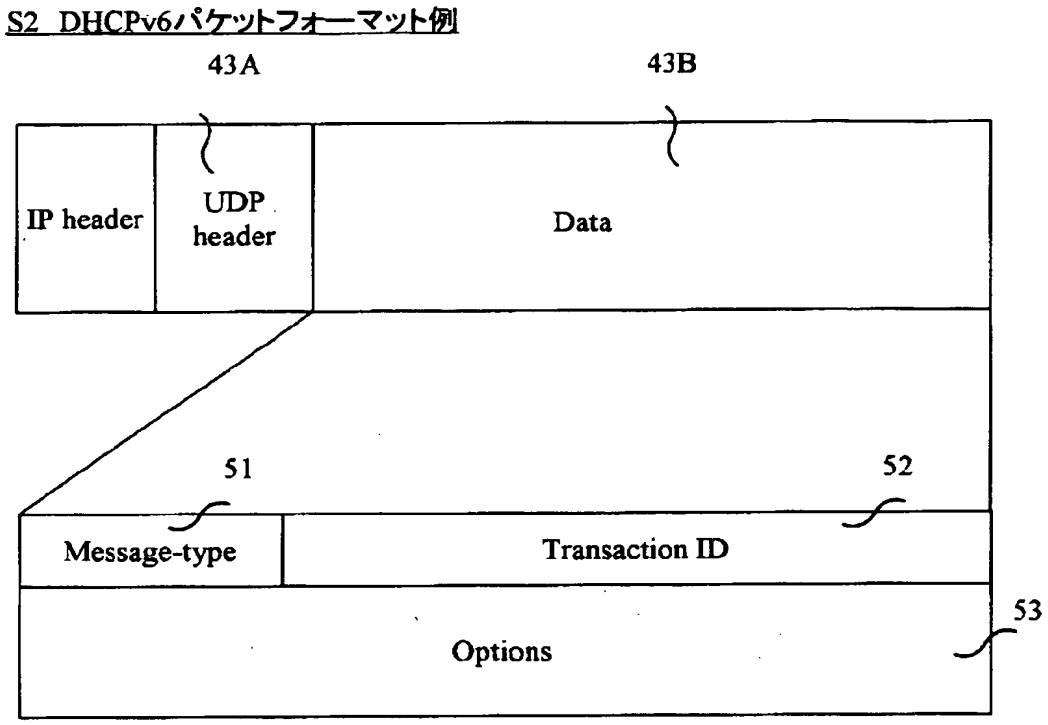
【図１１】

図11


S1 CMP メッセージ例
43A
43B
IP header
TCP header
Data
PKIMessage ::= SEQUENCE {
header PKIHeader,
body PKIBody,
protection [0] PKIProtection OPTIONAL,
extraCerts [1] SEQUENCE SIZE (1..MAX) OF Certificate OPTIONAL
}
S1

【図１２】

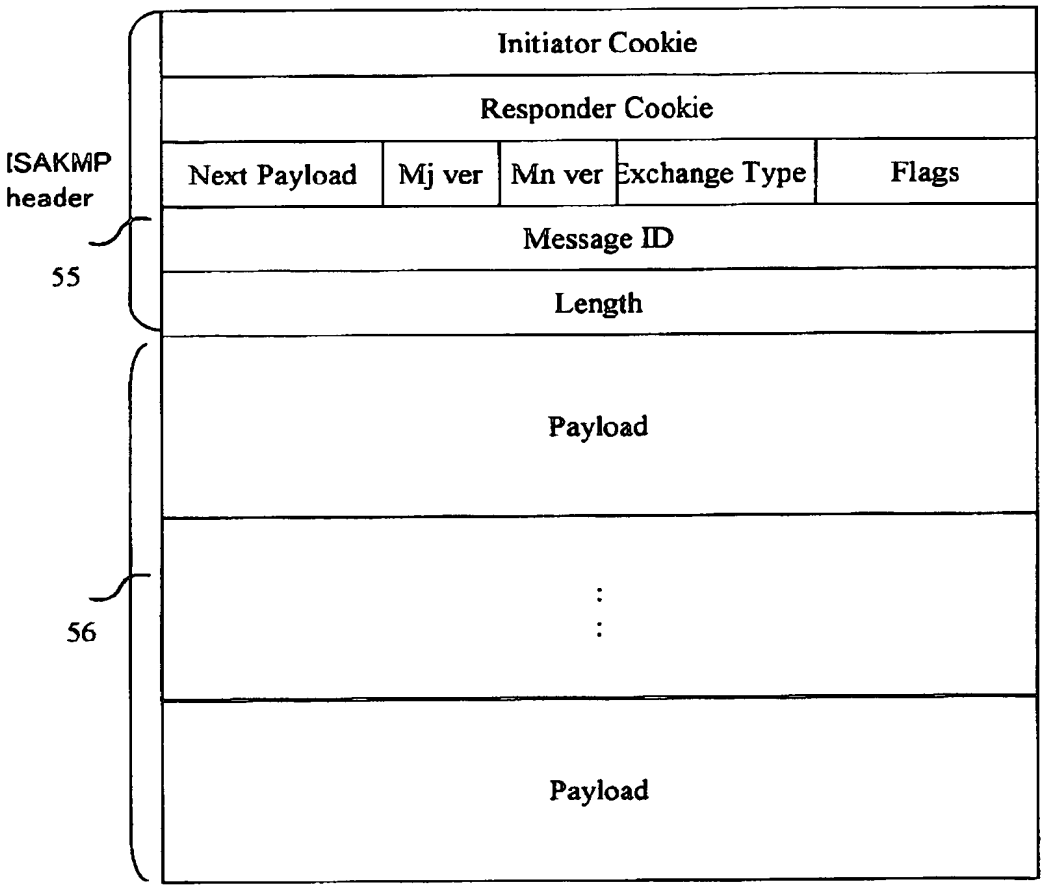
図12


S2 DHCPv6パケットフォーマット例
43A
43B
IP header
UDP header
Data
51
52
Message-type
Transaction ID
53
Options

【図１３】

図13

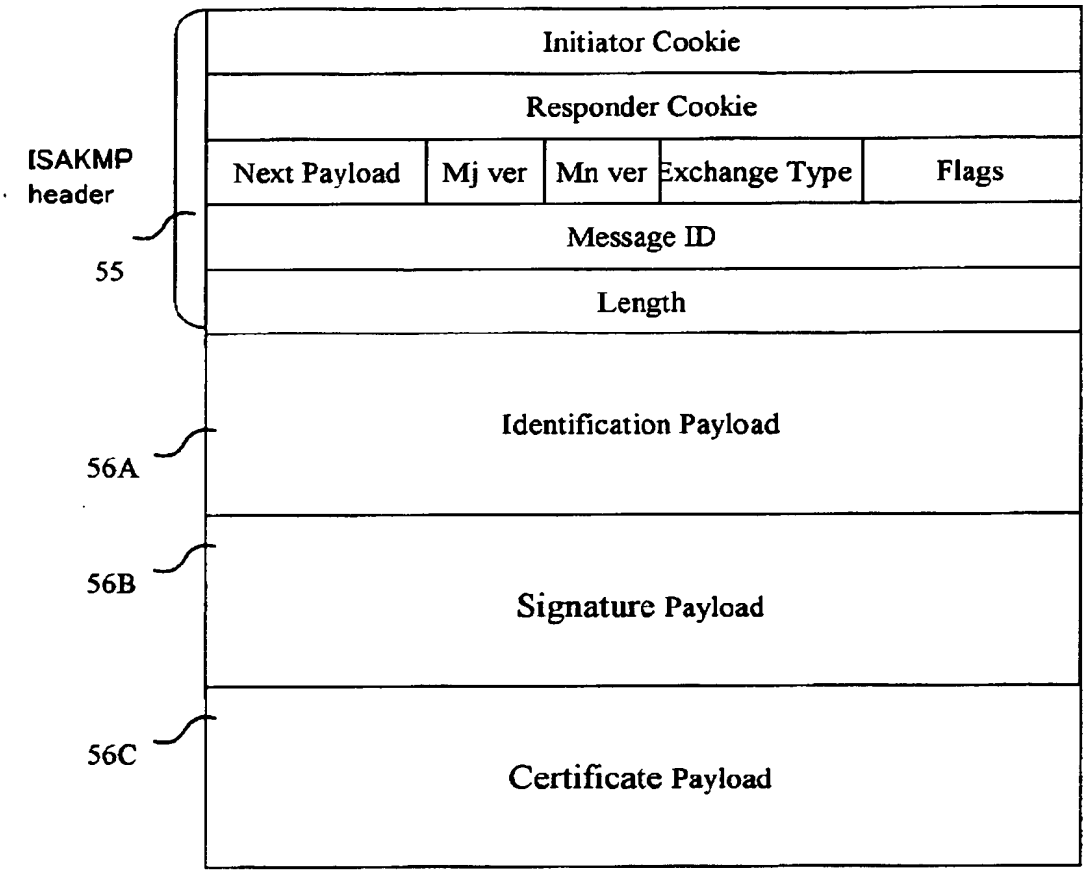
S3　ISAKMPパケットフォーマット例



【図１４】

図14

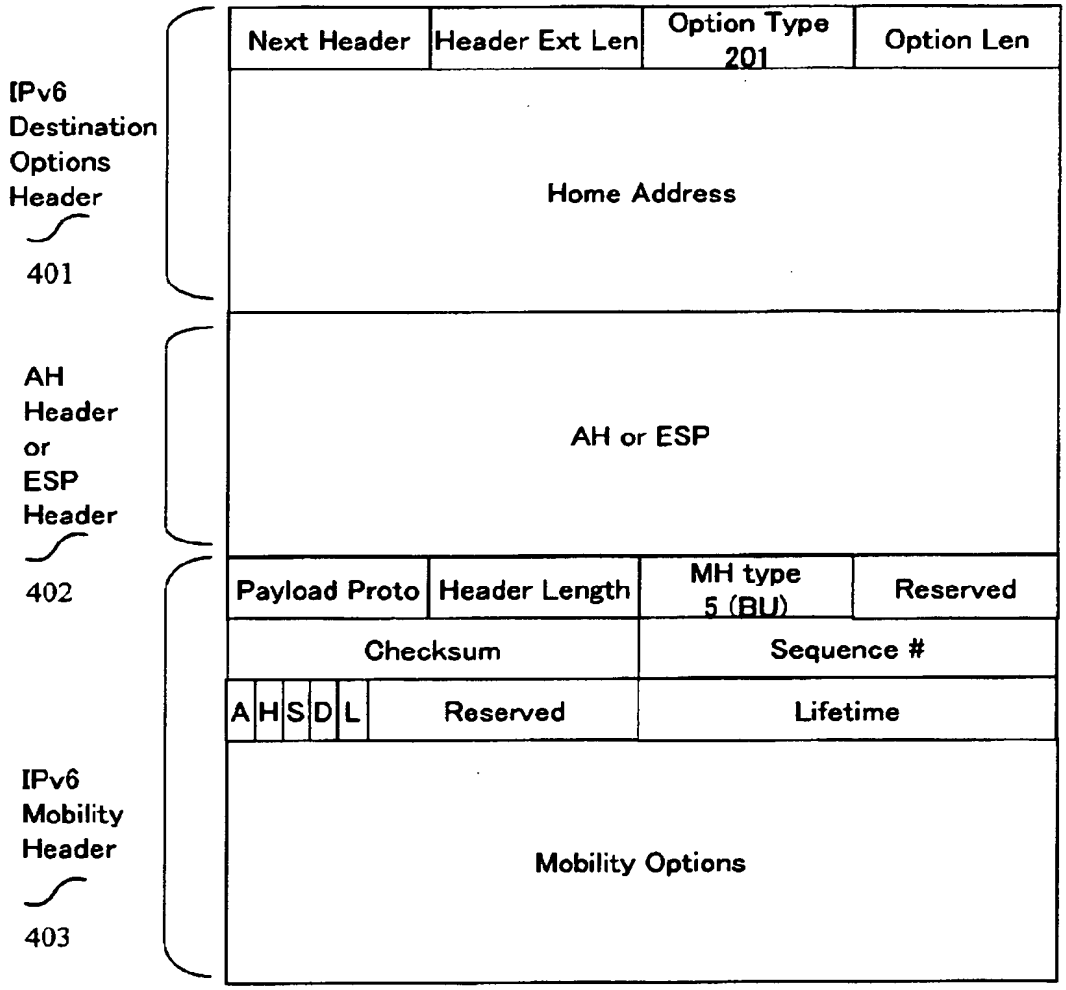
S4 ISAKMPパケットフォーマット例（IKEフェーズ1本人性確認）



【図１５】

図15

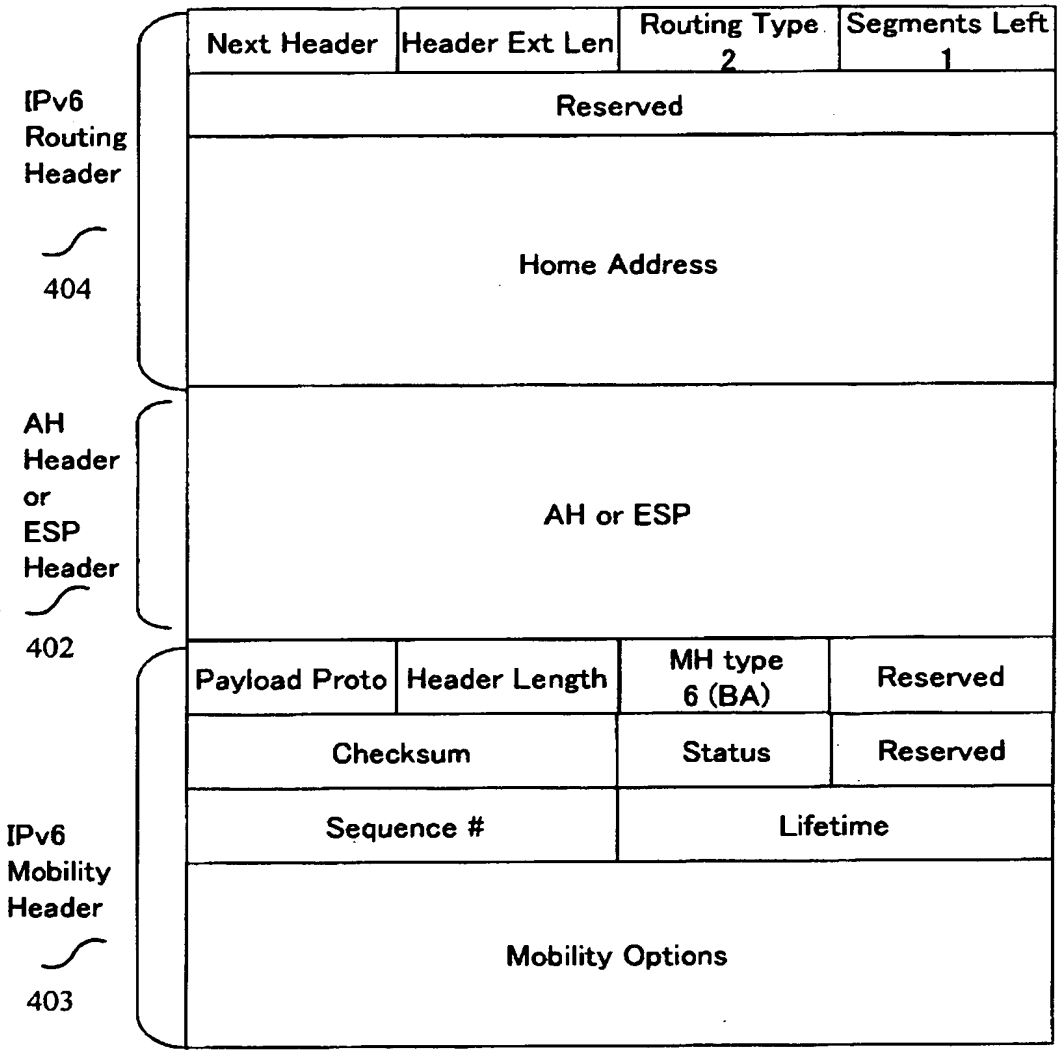
S11 Binding Updateメッセージフォーマット



【図１６】

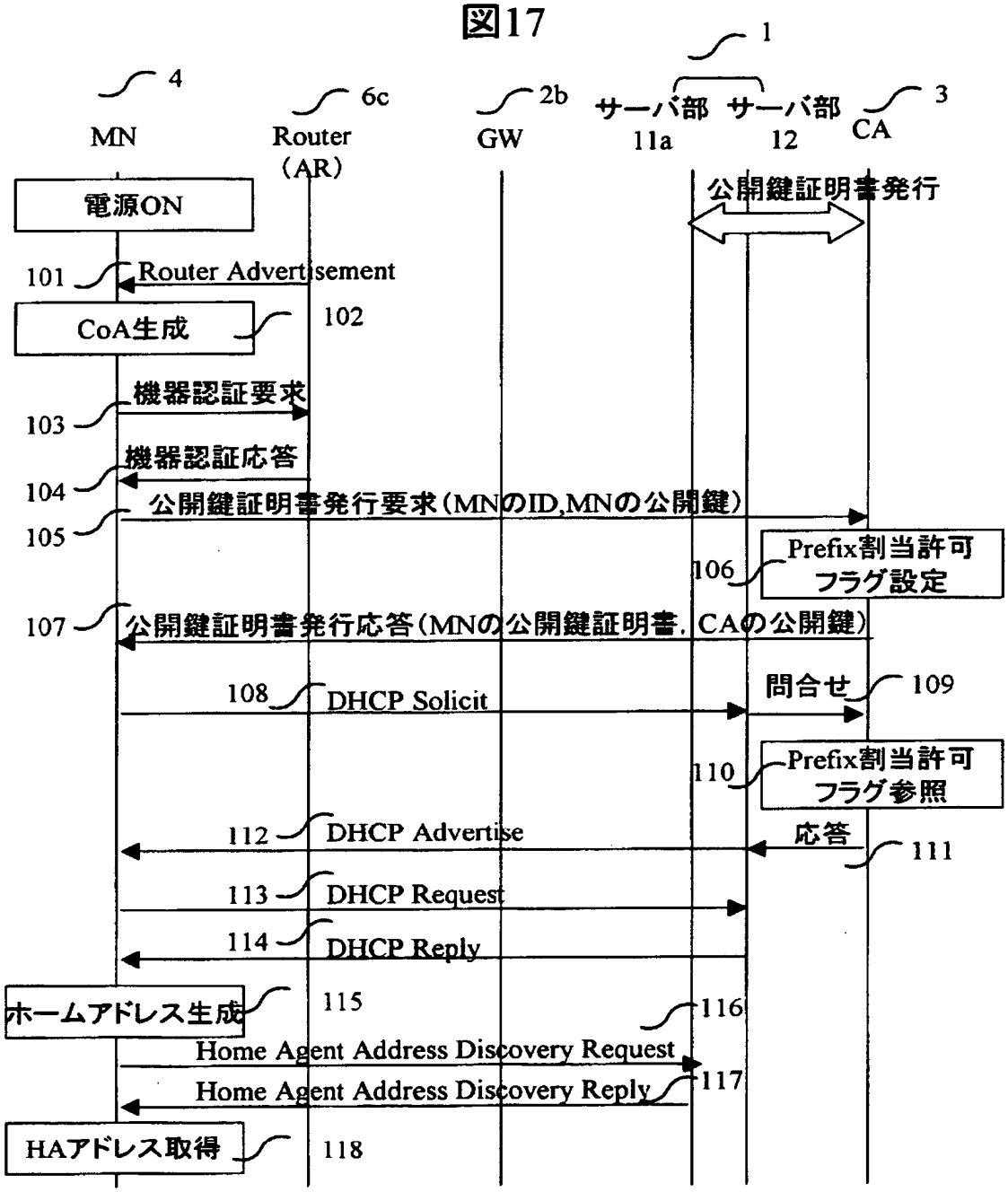
図16

S12 Binding Acknowledgementメッセージフォーマット



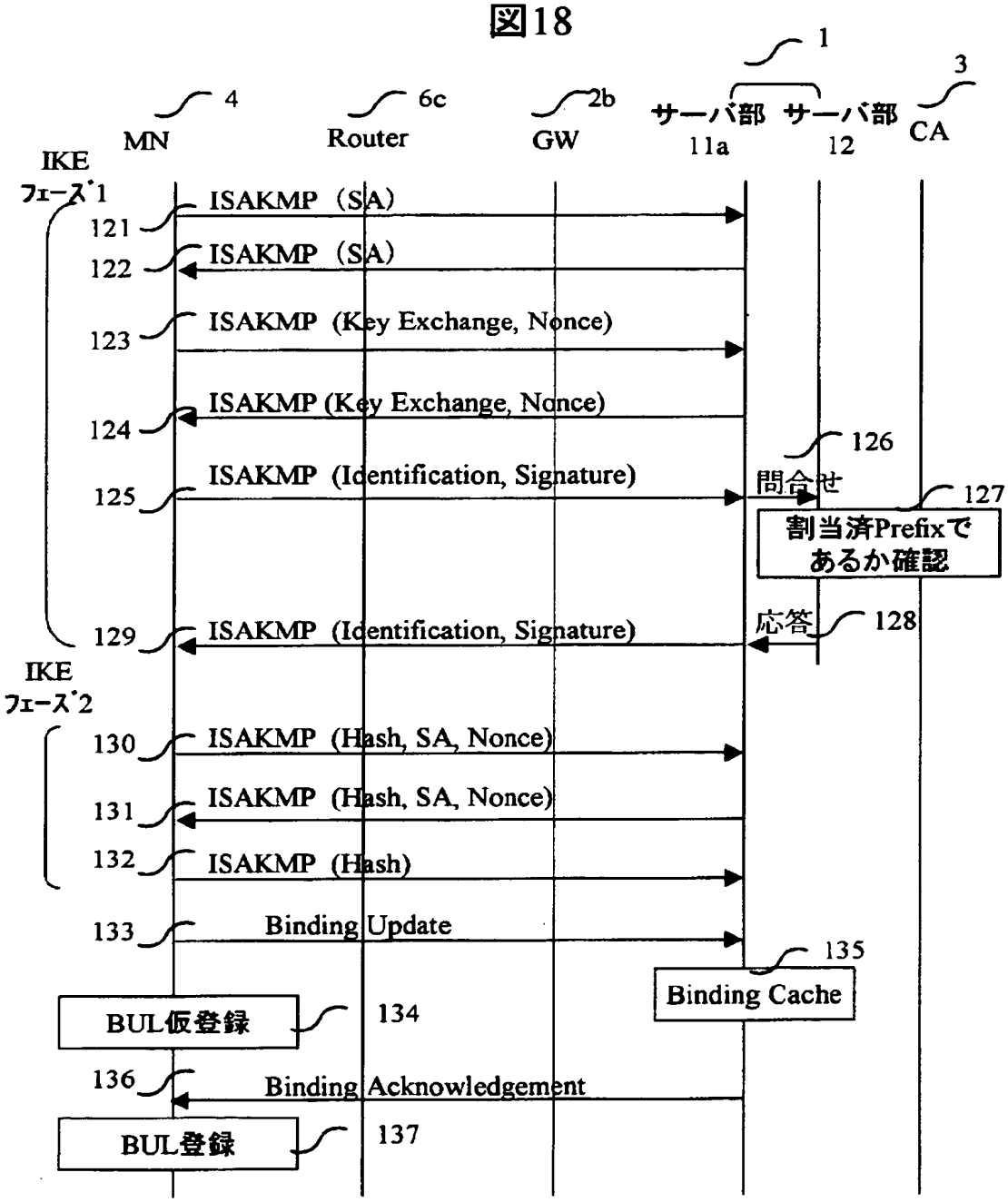
【図１７】

図17


1
4
6c
2b
3
MN
Router
(AR)
GW
サーバ部
11a
サーバ部
12
CA
公開鍵証明書発行
電源ON
101
Router Advertisement
CoA生成
102
機器認証要求
103
機器認証応答
104
公開鍵証明書発行要求(MNのID,MNの公開鍵)
105
106
Prefix割当許可
フラグ設定
107
公開鍵証明書発行応答(MNの公開鍵証明書, CAの公開鍵)
108
DHCP Solicit
問合せ
109
110
Prefix割当許可
フラグ参照
112
DHCP Advertise
応答
111
113
DHCP Request
114
DHCP Reply
ホームアドレス生成
115
116
Home Agent Address Discovery Request
117
Home Agent Address Discovery Reply
HAアドレス取得
118

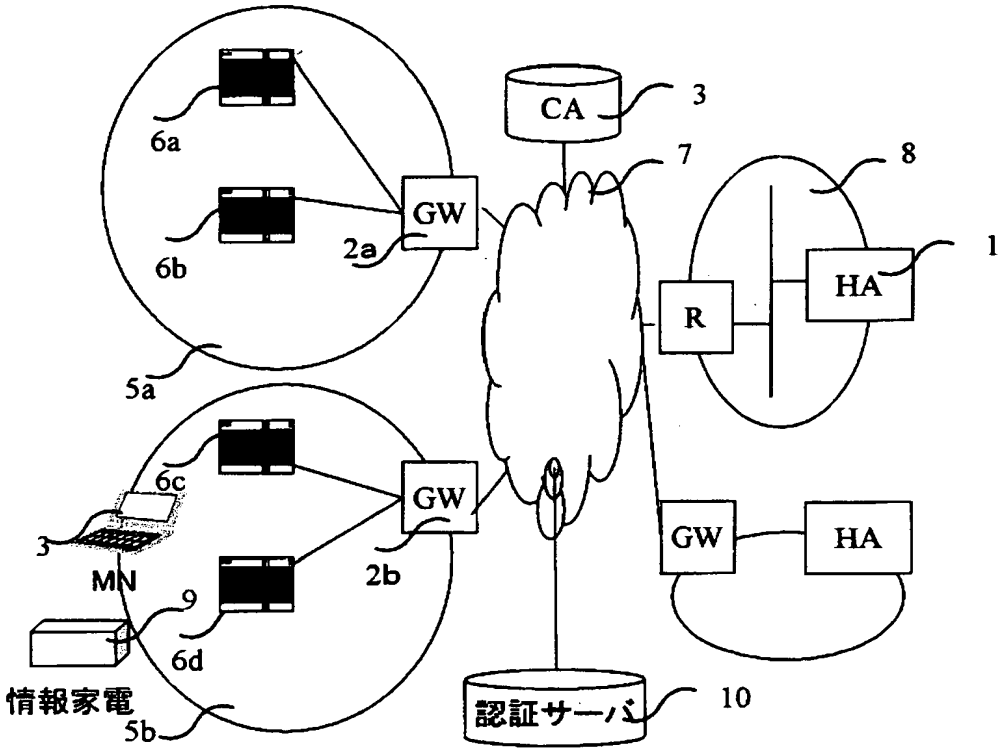
【図１８】

図18


1
3
4
6c
2b
サーバ部
サーバ部
CA
MN
Router
GW
11a
12
IKE
フェーズ1
ISAKMP (SA)
121
ISAKMP (SA)
122
ISAKMP (Key Exchange, Nonce)
123
ISAKMP (Key Exchange, Nonce)
124
126
ISAKMP (Identification, Signature)
125
問合せ
127
割当済Prefixで
あるか確認
応答
128
ISAKMP (Identification, Signature)
129
IKE
フェーズ2
ISAKMP (Hash, SA, Nonce)
130
ISAKMP (Hash, SA, Nonce)
131
ISAKMP (Hash)
132
Binding Update
133
135
Binding Cache
BUL仮登録
134
Binding Acknowledgement
136
BUL登録
137

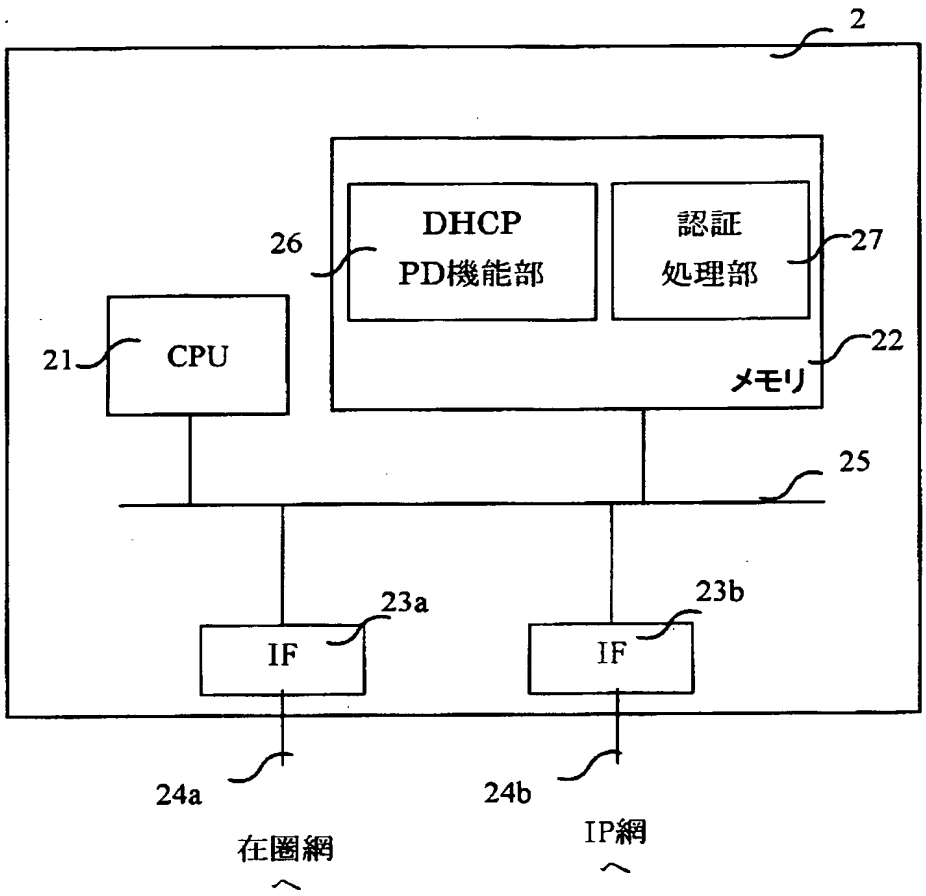
【図１９】

図19



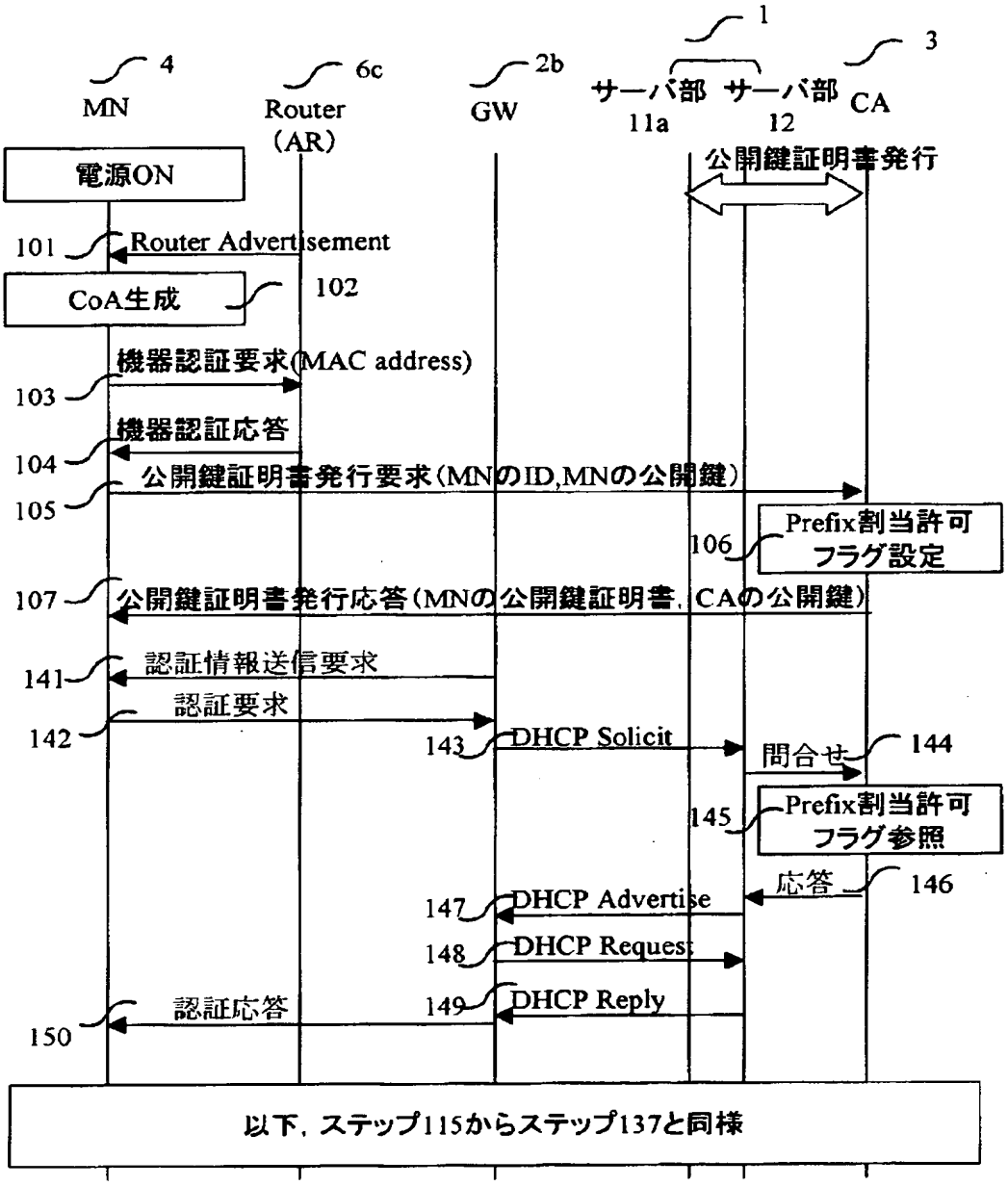
【図２０】

図20


2
DHCP
PD機能部
26
認証
処理部
27
21
CPU
メモリ
22
25
23a
IF
23b
IF
24a
24b
在圏網
へ
IP網
へ

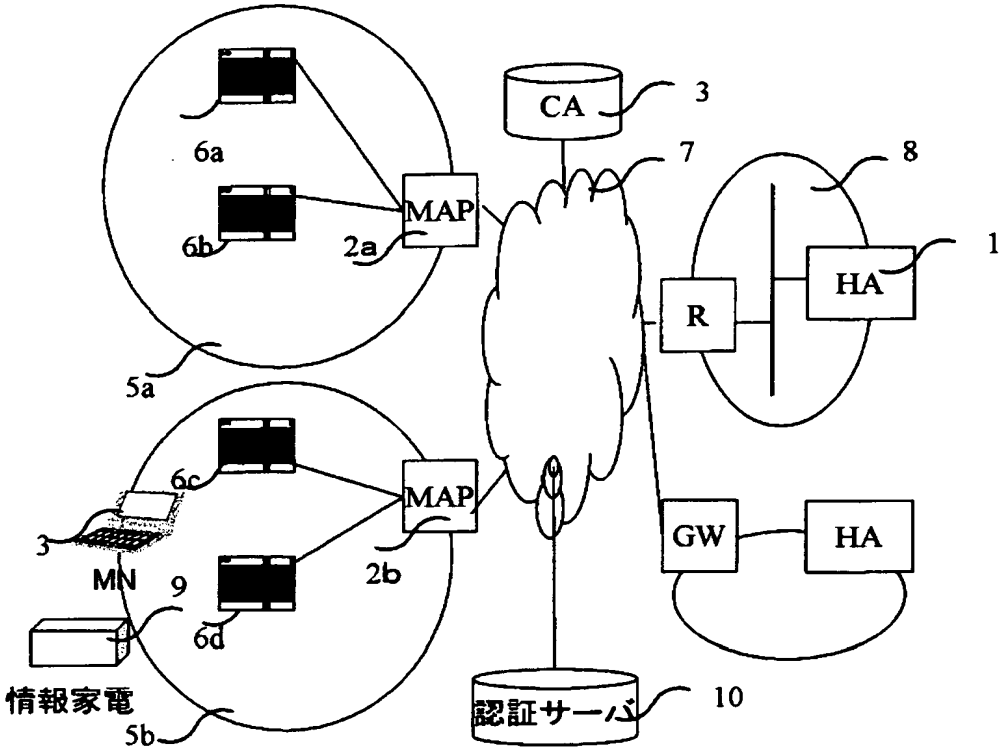
【図２１】

図21


1
3
4
6c
2b
MN
Router
(AR)
GW
サーバ部
11a
サーバ部
12
CA
公開鍵証明書発行
電源ON
101
Router Advertisement
CoA生成
102
機器認証要求(MAC address)
103
機器認証応答
104
公開鍵証明書発行要求(MNのID,MNの公開鍵)
105
106
Prefix割当許可
フラグ設定
107
公開鍵証明書発行応答(MNの公開鍵証明書, CAの公開鍵)
141
認証情報送信要求
142
認証要求
143
DHCP Solicit
問合せ
144
145
Prefix割当許可
フラグ参照
応答
146
147
DHCP Advertise
148
DHCP Request
149
DHCP Reply
150
認証応答
以下，ステップ115からステップ137と同様

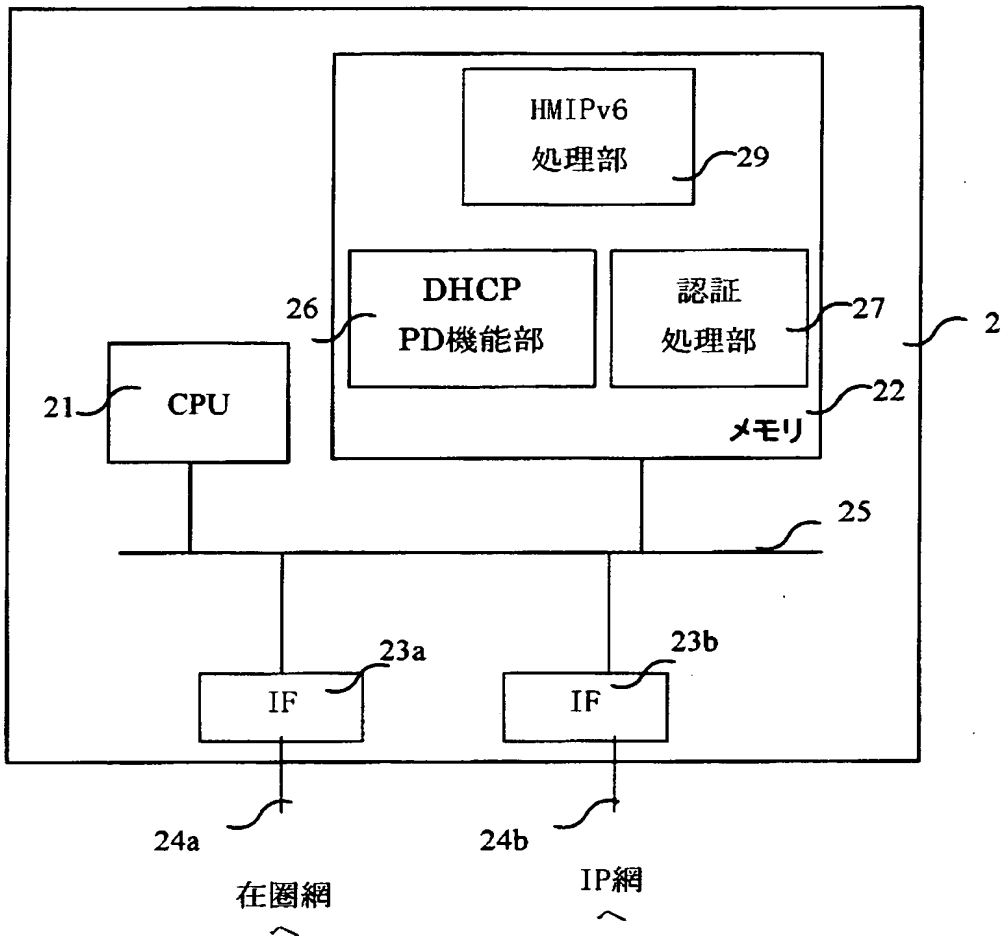
【図２２】

図22


CA
3
7
8
1
6a
MAP
6b
2a
HA
R
5a
6c
MAP
3
MN
9
2b
GW
HA
6d
情報家電
5b
認証サーバ
10

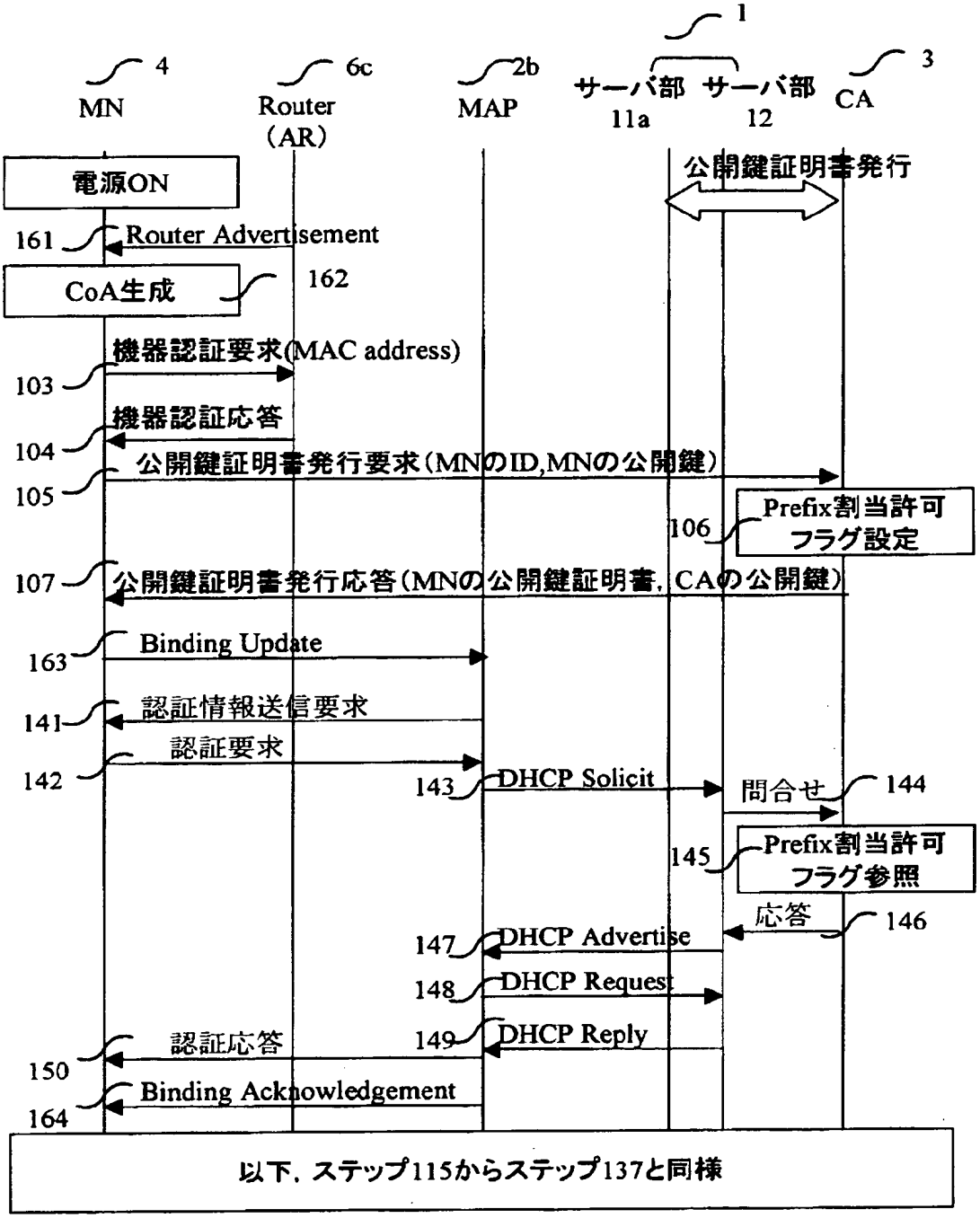
【図２３】

図23


HMIPv6
処理部
29
DHCP
PD機能部
26
認証
処理部
27
2
CPU
21
メモリ
22
25
23a
23b
IF
IF
24a
24b
在圏網
へ
IP網
へ

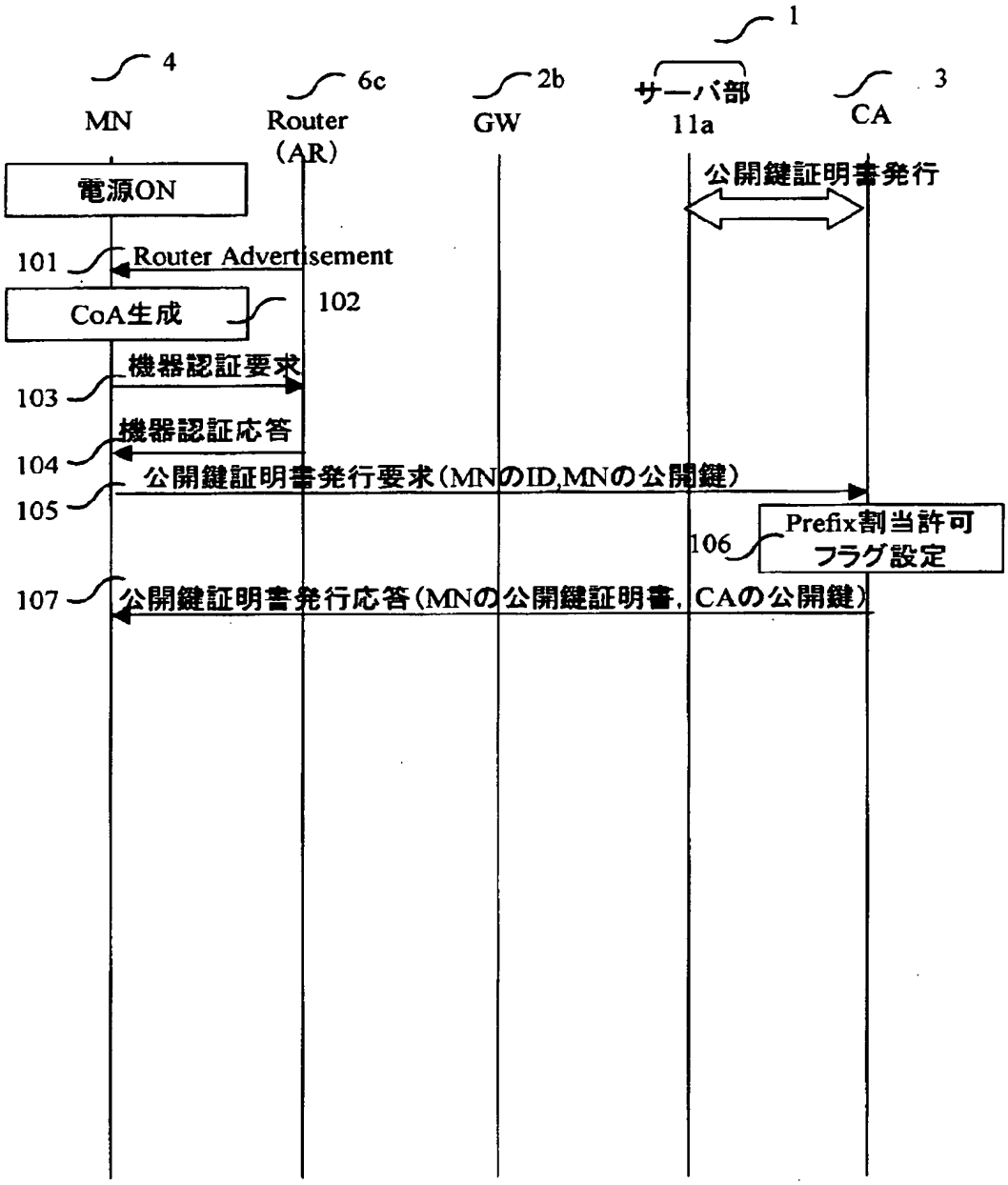
【図２４】

図24


1
4
MN
6c
Router
(AR)
2b
MAP
サーバ部
11a
サーバ部
12
3
CA
公開鍵証明書発行
電源ON
161
Router Advertisement
CoA生成
162
機器認証要求(MAC address)
103
機器認証応答
104
公開鍵証明書発行要求(MNのID,MNの公開鍵)
105
106
Prefix割当許可
フラグ設定
107
公開鍵証明書発行応答(MNの公開鍵証明書, CAの公開鍵)
163
Binding Update
141
認証情報送信要求
142
認証要求
143
DHCP Solicit
問合せ
144
145
Prefix割当許可
フラグ参照
応答
146
147
DHCP Advertise
148
DHCP Request
149
DHCP Reply
150
認証応答
164
Binding Acknowledgement
以下, ステップ115からステップ137と同様

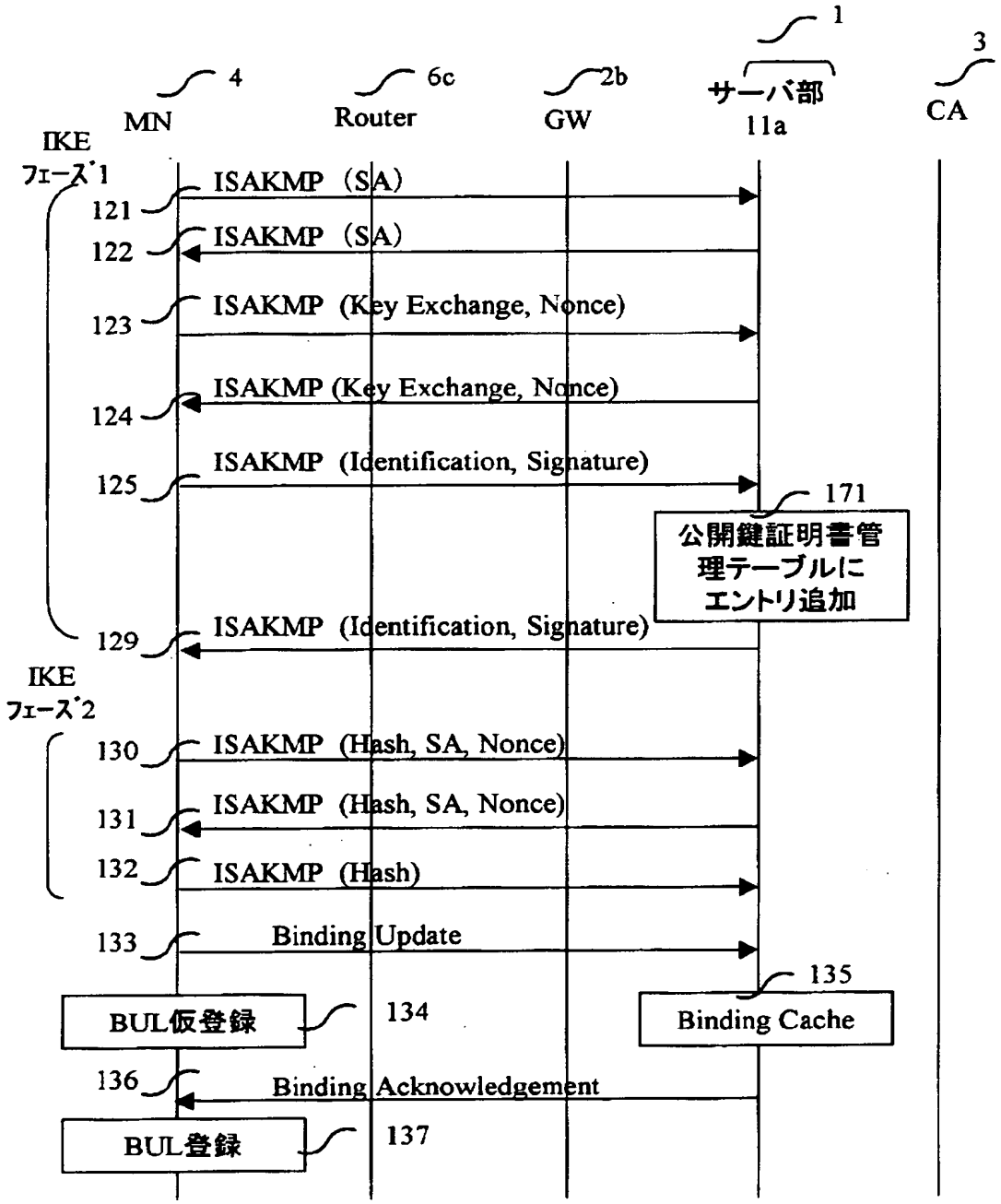
【図２５】

図25


1
4
6c
2b
サーバ部
3
MN
Router
(AR)
GW
11a
CA
公開鍵証明書発行
電源ON
101
Router Advertisement
CoA生成
102
機器認証要求
103
機器認証応答
104
公開鍵証明書発行要求(MNのID,MNの公開鍵)
105
Prefix割当許可
フラグ設定
106
107
公開鍵証明書発行応答(MNの公開鍵証明書, CAの公開鍵)

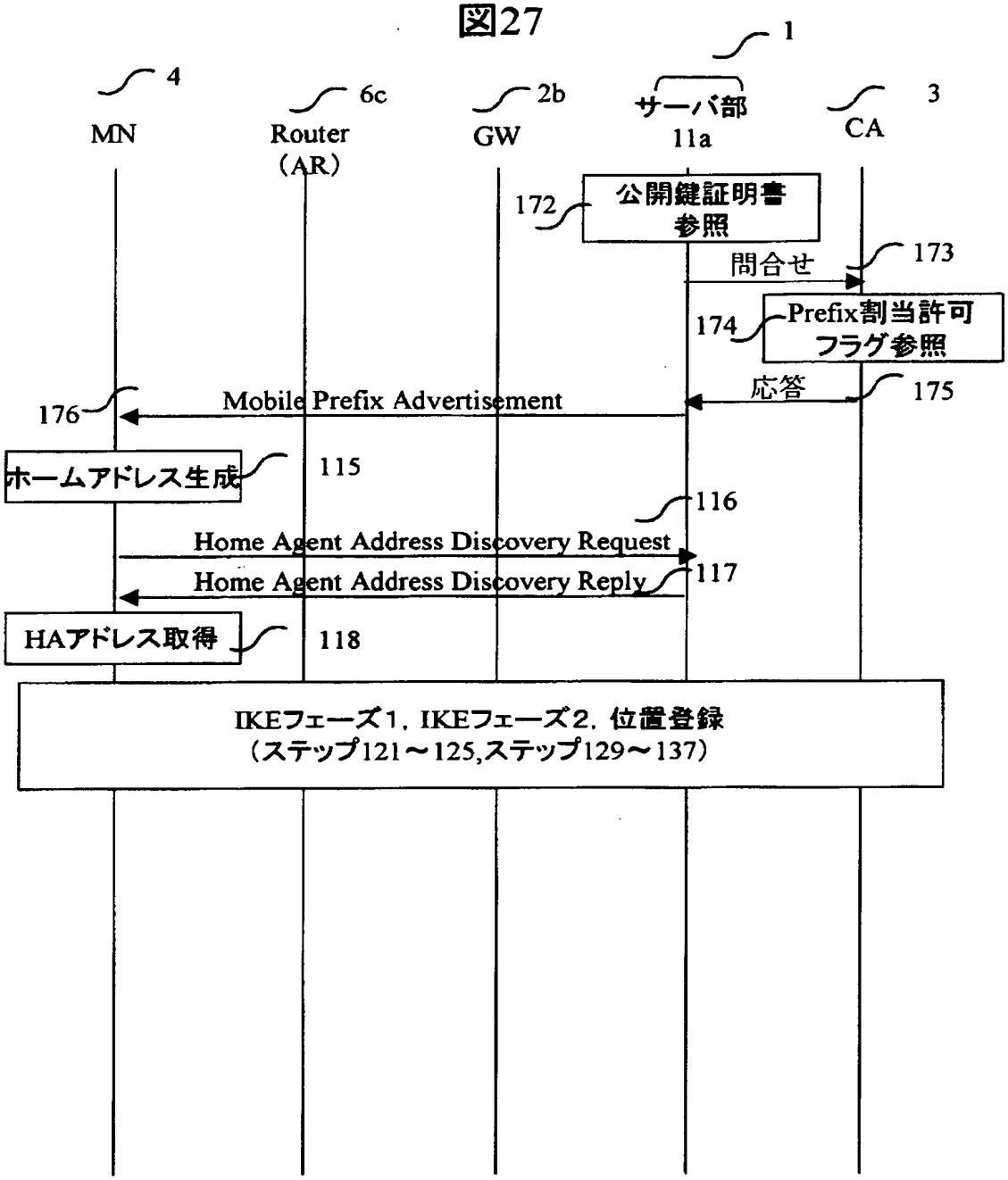
【図２６】

図26


1
3
4
6c
2b
サーバ部
MN
Router
GW
11a
CA
IKE
フェーズ1
ISAKMP (SA)
121
ISAKMP (SA)
122
ISAKMP (Key Exchange, Nonce)
123
ISAKMP (Key Exchange, Nonce)
124
ISAKMP (Identification, Signature)
125
171
公開鍵証明書管理テーブルにエントリ追加
ISAKMP (Identification, Signature)
129
IKE
フェーズ2
ISAKMP (Hash, SA, Nonce)
130
ISAKMP (Hash, SA, Nonce)
131
ISAKMP (Hash)
132
Binding Update
133
135
BUL仮登録
134
Binding Cache
Binding Acknowledgement
136
BUL登録
137

【図２７】

図27


1
4
6c
2b
サーバ部
3
MN
Router
(AR)
GW
11a
CA
172
公開鍵証明書
参照
問合せ
173
174
Prefix割当許可
フラグ参照
応答
175
176
Mobile Prefix Advertisement
ホームアドレス生成
115
116
Home Agent Address Discovery Request
Home Agent Address Discovery Reply
117
HAアドレス取得
118
IKEフェーズ1，IKEフェーズ2，位置登録
（ステップ121～125,ステップ129～137）

【書類名】　　要約書

【要約】

【課題】　Prefix通知機能やHAアドレス発見機能を使用する場合、MNのホームアドレスやHAアドレスが変更されるため、MNとHA間にIPsec SAを手動設定する方法は現実的ではない。また、現在のMobile IPv6にはMN自身を認証する機能がない。

【解決手段】　CA3はMN4に対するPrefix配布可否情報を保持する。HA１のサーバ部12はCA3が許可したMN4に対してPrefix情報を配布する。HA１のサーバ部11はMN4からIKEパケットを受信すると、サーバ部12にPrefix情報を確認後、IPsec SAを生成する。サーバ部11はIPsec SAを満たすMN4の位置登録要求を許容する。

【効果】　CA3が許可したMN4にPrefixを配布し、MN4が配布されたPrefixを用いてHA１との間にIPsec SAを生成することにより、MN4の正当性が確認できる。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－０６４３２９
受付番号	５０３００３８９５７０
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　３月１２日

＜認定情報・付加情報＞

【提出日】　平成15年 3月11日

次頁無

特願２００３－０６４３２９

出　願　人　履　歴　情　報

識別番号　　［０００００５１０８］

１．変更年月日　　１９９０年　８月３１日
［変更理由］　　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所